SUPREME COURT OF INDIA

CIVIL WRIT PETITION 829 / 2013

IN THE MATTER OF:

S.G. VOMBATKERE & ANR. ...PETITIONERS

Versus

UNION OF INDIA & ORS. ...RESPONDENTS

COMPILATION

VOLUME V - B

UIDAI & NPR DOCUMENTS

(Pages 217 - 394)

(See Inside for Complete Index)

Submitted on behalf of the Petitioners

VOLUME V

UIDAI & NPR DOCUMENTS

217

UIDAI

Unique Identification Authority of India
Planning Commission,
Yojana Bhavan,
Sansad Marg,
New Delhi 110001

Demographic Data Standards and Verification procedure (DDSVP) Committee Report

Version 1.0
December 9, 2009

Prepared by: DDSVP Committee

218

CONTENTS

219

LIST OF TABLES

1 Introduction

UIDAI has been setup by the Govt. of India with a mandate to issue a unique identification number to all the residents in the country. UIDAI proposes to create a platform to first collect the identity details and then to perform authentication that can be used by several government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identity in order to improve the efficacy of the service delivery. UIDAI has selected biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information is capable of carrying out the de-duplication at the time of collection of information. For government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that the biometric information capture and transmission are standardized across all the partners and users of the UID system.

The Government of India, in the past, had set up a number of expert committees for standards to be used for various e-governance applications in areas of Biometrics, Personal Identification and location Codification Standards. These committees have worked out standards in the respective categories to be uniformly applied for various e-governance standards.

As UIDAI proposes to use common demographic data for establishing and verifying identity, it becomes essential to standardize these fields and verification procedure across registrars and to aid interoperability across many systems that capture and work with resident identity.

1.1 Definitions and Acronyms

- UID – Unique Identification
- UIDAI – Unique Identification Authority of India
- Authority – Unique Identification Authority of India (UIDAI)
- DDSVP – Demographic Data Standards and Verification Procedure
- KYR – Know Your Resident
- KYC – Know Your Customer
- PoI – Proof of Identity
- PoA – Proof of Address
- DIT – Department of Information Technology
- ORGI – Office of Registrar General of India
- VARCHAR – Variable character string as represented in a database. Unlike the fixed-size character type, VARCHAR does not store any blank characters at the end, reducing the size of a database when the full length of the field is not used.
- UNICODE – Globally accepted standard definition of local language characters in a computer system. Character sets defined by Unicode Consortium.
- UTF-8 – Unicode Transformation Format, most widely used storage encoding for any UNICODE data

- Registrar – Any government or private agency that will partner with UIDAI in order to enroll and authenticate residents
- Introducer – A person who is authorized to introduce a resident who does not posses any supporting documents in order to help them establish UID (see later section 3.3 for details)
- Flag – a marker to indicate a particular status of a field

1.2 Committee Objective

A key requirement of the UID system is to capture necessary demographic data in a standardized manner so that this identity information works across various systems.

1. In order to achieve interoperability of data across various govt. and private agencies that will use the UID system, it is important that the capture and verification of basic demographic data for each resident is standardized across all partners of the UID system.
2. Another important aspect of demographic data collection is to ensure the correctness of the data at the time of enrolment of residents into the UID System. While an elaborate verification system based on local enquiries and existing documents issued by various agencies can be used to verify the correctness of the data to a large degree, it is likely to result into exclusion of poor and the marginalized who normally do not have any documents to prove their identity and addresses. As the main focus of the UIDAI is on inclusion, especially of the poor, the verification procedure has to be formulated in such a manner that while it does not compromise the integrity of the inputs, it also does not result in exclusion and harassment of the poor.
3. The government of India had set up expert committees for standards to be used for various e-governance applications in areas of Personal Identification, Biometrics, and Location Codification Standards. These committees have worked out few standards on the respective categories to be uniformly applied for various e-governance standards.
4. As UIDAI will use basic demographic data to establish identity and authentication, it becomes essential to review the applicability of the existing data and process standards for various e-Governance applications, modify them for UIDAI specific requirements and frame the methodology for its implementation.

In view of the above, a Demographic Data Standards and Verification Procedure (DDSVP) Committee was setup vide OM No.63/DG-UIDAI/2009 dated 09/10/2009 (annexed to this report) to review the existing standards and modify/enhance/extend them so as to achieve the goals and purpose of UIDAI.

1.3 Committee Charter

- To Recommend the Demographic Data standards (The data fields and their formats/structure etc.) that will ensure interoperability and standardization of basic demographic data and their structure used by various agencies that use the UID system. This will necessitate the review of the existing standards of Demographic

Data and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI and its partners.

- To Recommend the Process of Verification of these demographic data in order to ensure that the data captured, at the time of enrolment of the Residents into the UID system, is correct.

1.4 Target Audience

Any person or organization involved in designing, testing or implementing UID system, UID compatible systems, or UID enrollment for the central government, state government, commercial organizations, or any users of the UID system.

2 KYR Demographic Data

2.1 Introduction

Purpose of UIDAI is to help Residents establish their identity. So, it is important that the KYR data is kept to a usable minimum so as to support goals of UID and avoid other profiling and transactional fields.

2.1.1 Names and Addresses

Names in India can be from a single word to many (sometimes even 5 or more) words long depending on the region, caste, religion, etc. A standardized structure for names needs to be created for common KYR and interoperability between various systems.

Similarly, we neither have a standardized address format nor have well defined geographic boundaries beyond villages. This creates issues when trying to map addresses in a standard way. Various forms issued by existing registrars vary greatly when it comes to capturing addresses. As part of this committee, address structure for residents will also be standardized.

2.1.2 UID Number Format

The rationale for adopting UID numbering scheme was explained to the committee by UIDAI which is given below:

UID number is a 12-digit number with no intelligence built into it – it should be a random number, with as few digits as possible to accommodate the identification needs of the population for the next 100-200 years. UID number will be assigned only after biometric de-duplication process of the data supplied by the registrars.

The following factors were considered in order to arrive at a design of the UID number.

1. The date-of-birth and other attribute information should not be embedded in the UID number. Similarly, place of birth/residence using administrative boundaries (state/district/taluk) should not be embedded in the UID number. When state/district IDs are embedded in the UID number, the number faces the risk of becoming invalid and misleading the authenticator when people move from place to place. It can also lead to profiling/targeting based on the region/state/district that a person is from.

   The approach of storing intelligence in identification numbers was developed to make filing, manual search and book-keeping easier prior to the advent of computers. This is no longer necessary, since centralized database management systems can index the records for rapid search and access without having to section data by location or date of birth.

2. Given the rapid penetration of mobile phones and landlines across the country and across economic groups, the phone could become an enabling device used for authenticating a person, especially in the village scenario where internet penetration is still very small. In this case it would be useful to keep the UID number as a number rather than an alphanumeric.

3. Packing Density is the ratio of valid UID numbers issued to the total number of possible UID numbers available given a certain number of digits. The lower the packing density is, the more likely it is that a random guess will not produce a valid assigned UID number. In general it is suggested that we keep the packing density to about 20%.

4. The Authority intends to assign UID numbers to all residents – more than a billion people. UID number will not be re-used and hence numbering scheme need to accommodate necessary population growth over the years.

This committee has taken note of the above.

2.2 UID for Children

All children will be assigned a UID number. It is very important for several service organizations such as education and health to be able identify children uniquely in order to deliver services effectively. Children's' fingerprints are not fully formed and hence cannot be used for de-duplication given current state of technology.

Hence during enrollment, details of the parents are captured in order to link the child to established UIDs so that either of the parents can be used to authenticate the child. When the child's biometrics are well-formed (as per biometric committee recommendations), biometric capture will take place and the child will be de-duplicated to ensure the uniqueness of the child. Until the child is biometrically de-duplicated, their UIDs will be flagged as "De-duplication not performed".

2.3 Data Fields Summary

Information	Fields	Mandatory / Optional	Data Type
Personal Details	Name	Mandatory	Varchar (99)
	Date of Birth##	Mandatory	Date
	Gender	Mandatory	Char (1) – M/F/T
Address Details	Residential Address	Mandatory	8 address lines and pin code. See later sections for details.
Parent / Guardian Details	Father's/Husband's /Guardian's Name*	Conditional	Varchar (99)
	Father's/Husband's /Guardian's UID*	Conditional	Number (12)

	Mother's/Wife's /Guardian's Name*	Conditional	Varchar (99)
	Mother's/Wife's /Guardian's UID*	Conditional	Number (12)
Introducer Details	Introducer Name**	Conditional	Varchar (99)
	Introducer's UID**	Conditional	Number (12)
Contact Details	Mobile Number	Optional	Varchar (18)
	Email Address	Optional	Varchar (254)
## A flag is maintained to indicate if Date of Birth (DoB) is verified, declared, or approximate.			
** For infants, Father/Mother/Guardian's name (at least one) and UID is mandatory.* ** For children under a particular age, biometric de-duplication will not be done. Hence their UID will be flagged as such until they are biometrically de-duplicated at a later age (see section on UID for Children). Their UID will be linked to at least of the parent's UID.* ** For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is mandatory. But, an option will be provided to not specify in the case the adult is not in a position or does not want to disclose.*			
*** For residents with no document proof, an "introducer" should certify his/her identity. See later section on Introducer System.*			

Table 1: Data Fields Summary

2.4 Data Fields in Detail

2.4.1 Unique ID

Field Name	**UID**
Data Type	**Number (12)**
Mandatory / Optional	**Mandatory**
Specification Owner	UIDAI
Valid Values and Default Value	---
Language Support	---
Description	Internal generated random number. Unique in the whole system.
Display and Print Specifications	Print and display format should be **NNNN-NNNN-NNNN**

2.4.2 Name of Resident

Field Name	**NAME**
Data Type	**Varchar (99)**
Mandatory / Optional	**Mandatory**
Specification Owner	DIT (MDDS Standard)
Valid Values and Default Value	---
Language Support	Yes. Other than English, it will also be stored in one official Indian language. Data storage will be based in UTF-8. An additional Indian language code (Indian language codes as

	specified under DIT standards) will also be maintained for transliteration purposes. Specific guidelines such as handling "matras" on hand-written forms will be provided by UIDAI as part of registrar on-boarding process.
Description	Name of the resident.
Display and Print Specifications	---

2.4.3 Date of Birth

Field Name	**DOB**
Data Type	**Date**
Mandatory / Optional	**Mandatory**
Specification Owner	DIT (MDDS Standard)
Valid Values and Default Value	---
Language Support	---
Description	Date of Birth of the resident.
Display and Print Specifications	Print and display format should be **DD/MM/YYYY**

2.4.3.1 Date of Birth Type

Field Name	**DOB_TYPE**
Data Type	**Char (1)**
Mandatory / Optional	**Mandatory**
Specification Owner	DIT (MDDS Standard)
Valid Values and Default Value	"**V**" - Verified (full DoB as per document) "**D**" - Declared (full DoB as declared by resident) "**A**" -Approximate (Just the year, based on estimated age)
Language Support	---
Description	Flag used to indicate DoB type.
Display and Print Specifications	---

2.4.4 Gender

Field Name	**GENDER**
Data Type	**Char (1)**
Mandatory / Optional	**Mandatory**
Specification Owner	ORGI
Valid Values and Default Value	"**M**" – Male, "**F**" – Female, and "**T**" - Transgender
Language Support	---
Description	Gender of the resident
Display and Print Specifications	---

2.4.5 Residential Address

Field Name	**RESIDENTIAL_ADDRESS**
Data Type	**Address** (*see address structure details below*)
Mandatory / Optional	**Mandatory**
Specification Owner	Dept. of Post
Valid Values and Default Value	---
Language Support	Yes. Other than English, it will also be stored in one official Indian language. Data storage will be based in UTF-8. An additional Indian language code (Indian language codes as specified under DIT standards) will also be maintained for transliteration purposes.
Description	A verifiable address where resident lives normally.
Display and Print Specifications	Format should be (empty values/lines not printed): **C/o Person Name** **Building** **Street** **Landmark, Locality** **Village/Town/City, District** **State – Pin Code**

2.4.5.1 Address Structure

Address Field	Description	Data Type	Mandatory / Optional
CARE_OF	Field to capture "C/o" person name	**Varchar (60)**	Optional
BUILDING	Door/House/flat/Bldg number and name	**Varchar (60)**	Mandatory
STREET	Street number and name	**Varchar (60)**	Optional
LANDMARK	Major/Minor Landmark	**Varchar (60)**	Optional
LOCALITY	Locality/Area/Suburb /Sector/Block	**Varchar (60)**	Optional
VILLAGE_TOWN_CITY	Village/Town/City	**Varchar (8)** for code and **Varchar (50)** for name (stored as code*)	Mandatory
DISTRICT	District	**Varchar (4)** for code and **Varchar (50)** for name (stored as code*)	Mandatory
STATE	State	**Varchar (2)** for code and	Mandatory

		Varchar (50) for name (stored as code*)	
PINCODE	Postal code for an area	**CHAR(6)**	Mandatory
COUNTRY	Country. Currently not used on forms.	**Varchar (3)** for code and **Varchar (50)** for name (stored as code*)	Mandatory
** All region codes are based on "Land Codification" from ORGI*			

2.4.6 Father/Husband/Guardian and Mother/Wife/Guardian Information

Field Name	**NAME** and **UID**
Data Type	Same as Name and UID
Mandatory / Optional	**Name** of either Father/Husband/Guardian or Mother/Wife/Guardian **is mandatory for all.** But, **an option will be provided** to not specify in the case the adult is not in a position or does not want to disclose. In the case of **children,** both **Name and UID of at least one parent/guardian is mandatory.**
Specification Owner	DIT (MDDS Standard)
Valid Values and Default Value	---
Language Support	Yes. Other than English, it will also be stored in one official Indian language. Data storage will be based in UTF-8. An additional Indian language code will also be maintained for transliteration purposes.
Description	Name and UID of parent/guardian.
Display and Print Specifications	---

2.4.6.1 Relationship Type

Field Name	**RELATIONSHIP_TYPE**
Data Type	**Char (1)**
Mandatory / Optional	**Mandatory** when Parent/Spouse/Guardian data is provided
Specification Owner	UIDAI
Valid Values and Default Value	"**F**" – Father, "**M**" – Mother, "**H**" – Husband, "**W**" – Wife, and "**G**" – Guardian
Language Support	---
Description	Flag used to indicate. Two separate flags will be stored in database – one for Father/Husband/Guardian and another for Mother/Wife/Guardian.
Display and Print Specifications	---

2.4.7 Introducer Information

Field Name	**INTRODUCER_NAME** and **INTRODUCER_UID**
Data Type	**Varchar (99)** and **Number (12)**
Mandatory / Optional	**Optional**
Specification Owner	UIDAI
Valid Values and Default Value	---
Language Support	---
Description	In the case of residents having no documents as proof, they can be "introduced" by any approved "introducer" (see KYR process chapter for details on introducer system). **Both Name and UID will be captured in form although only Introducer UID will be stored against resident record.**
Display and Print Specifications	---

2.4.8 Mobile Number

Field Name	**RESIDENT_PHONE**
Data Type	**Varchar (18)**
Mandatory / Optional	**Optional**
Specification Owner	DIT (MDDS Standard)
Valid Values and Default Value	---
Language Support	---
Description	Mobile phone number of the resident. This can be used for enhanced authentication and alerting. Landline also will be accepted if mobile number is not available.
Display and Print Specifications	---

2.4.9 Email Address

Field Name	**RESIDENT_EMAIL**
Data Type	**Varchar (254)**
Mandatory / Optional	**Optional**
Specification Owner	DIT (MDDS Standard)
Valid Values and Default Value	---
Language Support	Yes.
Description	Email address of resident.
Display and Print Specifications	---

3 KYR Verification Procedure

3.1 Introduction

It is essential that key demographic data is verified properly so that the data within UID system can be used for authentication of identity by various systems. There are 3 distinct methods of verification:

- Based on supporting documents
- Based on introducer system (see section 3.5 for details)
- Based on the NPR (National Population Register) process of public scrutiny

All the above forms of verification are acceptable for UID enrollment.

At a high level the 'Personal Details' and the 'Address Details' are mandatory, whereas the 'Parent/Guardian', 'Introducer' and 'Contact' details are optional or conditional.

In order to verify the correctness of certain mandatory fields, such as Name, date-of-birth and address, there is a concept of 'Proof of Identity' (PoI) and "Proof of Address" (PoA). PoI requires a document containing the resident's name and photograph, whereas the PoA contains the name and address.

3.2 Broad Principles of Verification

One of the key goals of the UID system is to be inclusive and ensure every resident is able to establish their identity. There are certain key principles that verification procedure will follow to ensure inclusiveness without compromising data quality.

1. Ease of access
2. No harassment
3. No discrimination
4. No corruption
5. No exclusion

3.3 Verification Summary

Information	Fields	Verification Required?	Verification Procedure
Personal Details	Name	Yes	o Any of the PoI documents. o Introducer for people who have no documents.
	Date of Birth##	No	---
	Gender	No	---

Address Details	Residential Address (for UID letter delivery and other communications)	Yes	○ Any of the PoA documents. ○ Introducer for people who have no documents. ○ Address will be physically verified during UID letter delivery. But, resident's physical presence not required during letter delivery.
Parent / Guardian Details	Father's/Husband's /Guardian's Name*	Conditional	○ No verification of Father/Husband/Guardian in the case of adults.
	Father's/Husband's /Guardian's UID*		
	Mother's/Wife's /Guardian's Name*	Conditional	○ No verification of Mother/Wife/Guardian in the case of adults.
	Mother's/Wife's /Guardian's UID*		
Introducer Details	Introducer Name**	Yes	○ Introducer's Name, UID on the form. ○ Physical presence of the introducer at the time of enrollment may not be practical. UIDAI will therefore suggest alternate methods to overcome this practical difficulty.
	Introducer's UID**		
Contact Details	Mobile Number	No	---
	Email Address	No	---
## A flag is maintained to indicate if Date of Birth (DoB) is verified, declared, or approximate.			
* *For infants, Father/Mother/Guardian's name (at least one) and UID is mandatory. For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is mandatory.*			
** *For residents with no document proof, an "introducer" should certify his/her identity. See later section on Introducer System.*			

Table 2: Process Summary

3.4 KYR Guidelines

Following are the main guidelines for KYR process.

- **Uniform process** - A uniform procedure for KYR process & verification to be followed by each registrar that is easy to implement. Once a resident obtains a UID from any one of the registrars in the UID ecosystem; all other registrars will honor the validity of the UID fields obtained through the KYR process described in this document. This can eliminate cost involved in repeated KYR verification by several registrars.

- **Multiple options for supporting documents** - Applicants will be given a choice of supporting documents that they can produce as PoI and PoA. See later sections for supported list of documents.

- **Lack of Supporting Documents** – A process for enrolling residents who have no documented PoI and PoA must be defined through a concept of "Introducer". For details, please see section on Introducer System.

- **Supporting documents in regional languages** – The UID backend system will support the capture and storage of data in 2 languages – English and one official Indian language. Enrolling agencies must be prepared to verify and accept supporting documents that carry information in local languages.

- **Archiving Form & Supporting Documents** – Clarity in how the forms and supporting documents are archived for later access (dispute resolution, error in data entry etc) should be defined and followed across all enrolling registrars. Detail guidelines regarding this will be issued by UIDAI separately.

- **Accepting changes in demographic information** – Some of the fields captured during UID enrollment could change – such as Name and address. An update process will be supported in order to facilitate this. Upon following this process, the registrars will accept changes in demographic details. See later sections for details.

3.5 Introducer System

There are several situations, especially in the case of poor, where they are unable to provide any supporting documents. Since the main goal of UIDAI is inclusion, it is important that an effective process is developed to identify them and give a UID number without harassment.

An approach is to use a network of "approved" introducers who can introduce a resident and vouch for the validity of resident's information.

Essentially, this idea has been borrowed from the account opening procedure in the banks. When someone opens an account in the bank without any proofs, he/she needs an "introducer". This introducer is someone who already has an account in the branch and is ready to certify that X who wants to open the account is indeed X. Logically, then a branch has a chain of introducers. Every account that has been introduced is linked to the introducer.

This analogy needs to be generalized and expanded to become applicable to UID registration process. In the UID registration process, registration is proposed to be done through various registrars like the Banks, Insurance Companies, Central and State Government Departments. In each of these institutions, the introducer concept will work like a "tree structure" where one introducer may introduce more than one person. However, someone needs be the first introducer and be the "root" of this tree. The person at the root will be the person who will be "self-introduced". In other words, that

person will be initially registered without any introducer. He will then introduce and get a number of persons registered. This process will then continue.

As an example, in a registration process where State's Rural Development Department is the registrar and NREGA is the scheme whose beneficiaries are being registered. In this process, the District Magistrate (or the Deputy Commissioner) can "self-introduce" and become the root of the introducer tree. He/She will introduce his/her BDOs and the Block Panchayat heads (known as Block Pramukhs in some states) who implement NREGA. Each of these BDOs and Block Pramukhs can introduce other people at the Panchayat level like the Panchayat Sewaks, Pradhans/Mukhias (elected Panchayat Head), and ward members (in a village Panchayat). Generally, the last category will reach down to the village level. However, in order to ensure that the enrolment process is not hampered by the lack of approved introducers at the ground level, each registrar should have the freedom to decide on the issue of approved introducers so as to ensure that there are people at the ground level who are able to introduce the people who want to enroll in the UID system.

Similarly in a banking environment, senior bank officials will be able to introduce the lower functionaries and this will go down to the customer level.

In effect, there will be several approved 'introducers' who can help residents without supporting documents to enroll for a UID. Having multiple introducers within and outside government agencies should provide a needy resident access to people who can assert their identity while minimizing harassment. However, the concept of inclusiveness should not take away the credibility of the introducer system. As of now, offenses of impersonation (by the person) or abatement of this offense (by the introducer) should therefore be dealt with within the existing legal framework. However, UIDAI should put in place its own legal framework to deal with such situations as early as possible.

3.5.1 Goals of Introducer System

- Provide every resident having no documented proofs to provide an alternate method to confirm their identity and address.
- Ensure availability of multiple introducers so that residents are not being harassed by a single person.
- Since registrars provide the list of introducers, ensure that the introducer network spans people from Govt. and Private (e.g., Banks) and NGO agencies.
- Avoid disputes and fraud by making sure that introducers have their UID created before becoming an introducer and all introducers must be registered as such.

3.5.2 Broad Guidelines for Creating Introducers List

This section covers broad guidelines that can be used by registrars for creating a list of introducers within their domain. Following are some of the guidelines:

- The list of approved introducers should go down till the village/customer level so that the process of registration is not hampered due to lack of introducers.

- The registrars need not keep the hierarchy of approved introducers limited to their own department/organization. As an example, in NREGA, there are a number of NGOs involved in NREGA social audit and the registrars could make some of the representatives of these NGOs who work at the village level as the approved introducers. Similarly, the village teachers and postman could also be incorporated as approved introducers by state Governments if required.
- At the ground level, residents should have access to multiple introducers so as to avoid harassment by a single introducer.
- Introducer list should include credible organizations which have traditionally been advocates of vulnerable communities to make sure goal of inclusion is truly achieved.

3.5.3 Introducer System in Detail

As discussed earlier, UIDAI will request registrars to provide a list of people who can act as trusted introducers within their ecosystem. It is highly recommended that this list includes people from both government and private enterprises including NGOs if necessary so that residents get a choice of people to approach for getting the introduction done. UIDAI may also provide its own list of introducers to make the pool of introducers large enough.

All introducers are required to be enrolled into UID system and obtain their UID number before they can become an introducer. This helps in effectively auditing all introductions.

Residents with no document proofs can approach any of the introducers enlisted to assert their identity. Residents are required to fill up the enrollment form and take it to one of the introducers for getting introduced. Introducer will verify the information filled, fill up his/her name and UID, and put thumb impression within the specified area of the form.

UIDAI should, in consultation with its various Registrars, come out with a detailed policy and guideline for the Introducer. This will be in the form of a Manual to be followed by the various stakeholders.

3.6 Supporting Documentation

During enrolment, the quality of data has to be ensured primarily with supporting documents that the resident provides. Copies of documents provided will be verified against the original. Physical copies of the documentary evidence will be stored by the Registrar and available for audit by the designated audit agencies.

In the case of residents with no documentation, introducer system can be used to enroll them into the system.

UIDAI and Registrars shall have the authority to amend and enlarge the list of PoI and PoA documents as and when necessary.

3.6.1 Proof of Identity (PoI) Documents

Proof of Identity document **must contain name and photo** of the resident. Any of the following PoI documents are supported:

Supported PoI Documents Containing Name and Photo
1. Passport 2. PAN Card 3. Ration/PDS Photo Card 4. Voter ID 5. Driving License 6. Government Photo ID Cards 7. NREGS Job Card 8. Photo ID issued by Recognized Educational Institution 9. Arms License 10. Photo Bank ATM Card 11. Photo Credit Card 12. Pensioner Photo Card 13. Freedom Fighter Photo Card 14. Kissan Photo Passbook 15. CGHS / ECHS Photo Card 16. Address Card having Name and Photo issued by Department of Posts 17. Certificate of Identity having photo issued by Group A Gazetted Officer on letterhead

Table 3: PoI Documents

NOTE: *If any of the above documents submitted do not contain the photograph of the resident, then it will not be accepted as a valid PoI. In order to be inclusive and free of harassment, documents with older photographs are acceptable.*

3.6.2 Proof of Address (PoA) Documents

Proof of Address document **must contain name and address** of the resident. Any of the following PoA documents are supported:

Supported PoA Documents Containing Name and Address
1. Passport 2. Bank Statement/Passbook 3. Post Office Account Statement/Passbook 4. Ration Card 5. Voter ID 6. Driving License 7. Government Photo ID Cards

8. Electricity Bill (not older than 3 months) 9. Water Bill (not older than 3 months). 10. Telephone Landline Bill (not older than 3 months) 11. Property Tax Receipt (not older than 3 months) 12. Credit Card Statement (not older than 3 months) 13. Insurance Policy 14. Signed Letter having Photo from Bank on letterhead 15. Signed Letter having Photo issued by registered Company on letterhead 16. Signed Letter having Photo issued by Recognized Educational Institution on letterhead 17. NREGS Job Card 18. Arms License 19. Pensioner Card 20. Freedom Fighter Card 21. Kissan Passbook 22. CGHS / ECHS Card 23. Certificate of Address having photo issued by MP or MLA or Group A Gazetted Officer on letterhead 24. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas) 25. Income Tax Assessment Order 26. Vehicle Registration Certificate 27. Registered Sale / Lease /Rent Agreement 28. Address Card having Photo issued by Department of Posts 29. Caste and Domicile Certificate having Photo issued by State Govt.

Table 4: PoA Documents

3.6.3 Proof of Date of Birth (DoB) Documents

Proof of DoB document **must contain name and DoB** of the resident. Any of the following documents are supported:

Supported Proof of DoB Documents
1. Birth Certificate 2. SSLC Book/Certificate 3. Passport 4. Certificate of Date of Birth issued by Group A Gazetted Officer on letterhead

Table 5: Proof of DoB Documents

3.7 KYR Process

3.7.1 Verifying Name

Name must be verified against any one of the PoI documents listed. A copy of PoI should be kept as part of enrollment and verification should be done against the original document.

In the case of resident not having a valid PoI document, resident should furnish the form signed by any of the approved introducers.

3.7.2 Verification for Name Change

Residents may want to change his/her name due to various reasons. Name change should be verified against documents. Following are the reasons and verification method for supporting name changes.

Marriage

Women may want to change their name after marriage. In this case, a copy of the marriage certificate or any acceptable proof of marriage as approved by the registrar should be provided and should be verified against original documents.

Any Other

Residents may change their name for other reasons such as self-wish, religion change, numerology, etc. In all these cases, they should provide a copy of legal name change certificate and it should be verified against the original document.

3.7.3 Verifying DoB

Date of Birth should be verified against any of the Proof of DoB documents listed above. Copy of the document should be verified against the original.

In the case of lack of documents, an approximate DoB may be taken and marked as so.

3.7.4 Verifying Address

The addresses will be verified against any one of the PoA documents listed. A copy of PoA document should be kept as part of enrollment and verification should be done against the original document.

In the case of resident not having a valid PoA document, resident should furnish the form signed by any of the approved introducers.

3.7.5 Verification for Address Change

Residents can update their address through any of the enrolling registrars. Process for address verification is same as described above.

3.7.6 Verifying Parents/Spouse/Guardian Information

In the case children, "Name" and "UID" of one of the parents or guardian is mandatory. Parent/Guardian must bring their UID letter when enrolling children (or they can be enrolled together) and should be verified.

In the case of an adult, no verification will be done for the information on parent or spouse. They are recorded for internal purposes only.

3.7.7 Making Corrections to Initial Data

In the case of mistakes such as spelling errors, address errors, etc. resident should be able to come back and request such corrections. Enrolling agencies should allow making those changes based process similar to initial KYR.

3.8 Exceptions Handling

There are likely to be several types of exceptions during enrolment process that need to be handled. Following list provide the common exceptions and appropriate verification method.

Exception	Process
DoB Unknown	Record estimated year of birth leaving date and month fields. DoB Type flag set to "Approximate".
Inconsistent Address in PoA document	Quite like name spelling errors, address too is likely to have a large number of inconsistencies across documents. Addresses must be mapped appropriately onto the standard KYR address fields as per specification.
Absence of original documents	In instances where original documents are not available, copies attested / certified by a public notary / gazetted officer will be accepted.

Table 6: KYR Exceptions List

UIDAI shall have the right to alter / amend the guidelines in this regard from time to time.

4 References

1. ***"Person Identification Codification (MDDS), Version 1.02"*** – by Expert Committee on Metadata and Data Standards, DIT (http://egovstandards.gov.in/).
2. ***"Land Region Codification, Version 1.02"*** – by Expert Committee on Metadata and Data Standards, DIT (http://egovstandards.gov.in/).
3. ***"Master Circular – Know Your Customer (KYC) norms"*** – by RBI (http://rbidocs.rbi.org.in/rdocs/notification/PDFs/73IKYC010709_F.pdf)
4. ***"UPU S42 International Address Standard"*** – by UPU (http://www.upu.int/). Also see the reference article at http://xml.coverpages.org/ni2003-06-17-a.html
5. ***"Customer Information Quality Specifications Version 3.0"*** – by OASIS (http://docs.oasis-open.org/ciq/v3.0/specs/ciq-specs-v3.html)
6. ***"Markup Languages for Names and Addresses"*** – OASIS Cover Pages (http://xml.coverpages.org/namesAndAddresses.html)

5 Members

5.1 DDSVP Committee

S.No.	Name & Designation	Role
1	Mr. N. Vittal, Former CVC	Chairman
2	Mr. S. R. Rao, Additional Secretary, DIT	Member
3	Dr. C. Chandramauli, RGI	Member
4	Mr. K. Raju, Principal Secretary, Rural Development, GoAP, Hyderabad	Member
5	Dr. DS Gangwar, Jt Secy., Min of Rural Development, New Delhi	Member
6	Shri Ram Narain, DDG(Security), Dept. of Telecommunication	Member
7	Mr. Vinay Baijal, CGM (DBoD), RBI, Mumbai	Member
8	Mr. VS Bhaskar, Commissioner & Secretary, Health & FW, IT, Sports & Youth Welfare, Government of Assam, Guwahati	Member
9	Mr. S. Satpathy, Secretary, Rural Development, Govt of Jharkhand, Ranchi	Member
10	Ms. Kalpana Tiwari, Department of Posts	Member
11	Prof. Bharat Bhaskar, IIM, Lucknow	Member
12	Mr. Ashutosh Dixit, Jt. Secretary (TPL II), Dept. of Revenue	Member
13	Ms. Madhavi Puri Buch, ICICI Securities, Mumbai	Member
14	Dr. Gayathri V., CEO LabourNet	Member
15	Mr. Ram Sewak Sharma, DG UIDAI	UIDAI Rep.
16	Mr. Srikanth Nadhamuni	UIDAI Rep.
17	Dr. Pramod K. Varma	UIDAI Rep.

5.2 KYR Data Sub-committee

S.No.	Name & Designation	Role
1	Shri S.R. Rao, Additional Secy. DIT	Chairman
2	Shri Ashutosh Dixit, JS Dept. of Revenue	Member
3	Shri Chakravarty DDG, RGI Office	Member
4	Dr. D.S. Ganwar, JS, MoRD	Member
5	Shri V.S. Bhaskar, Commissioner and Secy, Health and Family welfare, Govt. of Assam	Member
6	Ms. Renu Bhudiraja, Director, DIT	Member
7	Ms. Aruna Chaba, Senior Technical Director, NIC	Member
10	Shri Ram Sewak Sharma, DG UIDAI	UIDAI Rep.
11	Shri Srikanth Nadhamuni	UIDAI Rep.
12	Dr. Pramod K. Varma	UIDAI Rep.

5.3 KYR Process Sub-committee

S.No.	Name & Designation	Role
1	Ms. Kalpana Tiwari, India Post	Chairman
2	Shri Ram Narain, Joint Secy. DoT	Member
3	Dr. D.S. Ganwar, JS, MoRD	Member
4	Shri V.S. Bhaskar, Commissioner and Secy, Health and Family welfare, Govt. of Assam	Member
5	Shri Ashutosh Dixit, JS Dept. of Revenue	Member
6	Prof. Bharat Bhaskar, IIM Lucknow	Member
10	Shri Ram Sewak Sharma, DG UIDAI	UIDAI Rep.
11	Shri Srikanth Nadhamuni	UIDAI Rep.
12	Dr. Pramod K. Varma	UIDAI Rep.

9.12.09

(N. Vittal)
Chairman, DDSVP Committee

242

UIDAI

Unique Identification Authority of India
Planning Commission,
Yojana Bhavan,
Sansad Marg,
New Delhi 110001

Biometrics Design Standards For UID Applications

Version 1.0
December 2009

Prepared by: UIDAI Committee on Biometrics

243

CONTENTS

1 Executive Summary

The Unique Identification Authority of India (UIDAI) was set up by the Govt. of India on 28 January 2009. The purpose of the UIDAI is to issue Unique Identification numbers to all residents in the country. The Authority set up a Biometrics Standards Committee in order to frame biometrics standards for use by the UIDAI and its partners. The first deliverable of the Committee was to frame biometric standards based on existing national and international standards, with the consensus of various government stakeholders. The second deliverable was to recommend appropriate biometrics parameters to achieve the UIDAI's mandate. The second goal of the Committee encompasses best practices, expected accuracy, interoperability, conformity and performance in biometrics standards.

After reviewing international standards and current national recommendations, the Committee concluded that the ISO 19794 series of biometrics standards for fingerprints, face and iris set by the International Standards Organization are the most suitable. These standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics. The standards framed for the UIDAI are accordingly, fully compliant with the respective ISO standards, and are given in Sections 7 through 11.

The Committee notes that Face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. The fingerprint industry also has a variety of suppliers and a base of experienced professionals necessary to implement the unique identity management solution at the scale that India requires. Based on these factors, the Committee recognises that a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts.

The Committee however, is also conscious of the fact that de-duplication of the magnitude required by the UIDAI has never been implemented in the world. In the global context, a de-duplication accuracy of 99% has been achieved so far, using good quality fingerprints against a database of up to fifty million. Two factors however, raise uncertainty about the accuracy that can be achieved through fingerprints. First, retaining efficacy while scaling the database size from fifty million to a billion has not been adequately analyzed. Second, fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context.

The Committee therefore held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group was also formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all the images were from rural regions, and were collected by different agencies using different capture devices, and through different operational processes. The analysis reported in Section 12.4 and the associated Annexure show that the UIDAI could obtain fingerprint quality as good as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is

data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

The demographic data (non-biometric data) is also used for improving de-duplication processes. It reduces the amount of manual labor required to establish genuine duplicates from a possible list of duplicate matches.

Further, it has also been observed that Iris, which for a long period of time was under the proprietary domain, is emerging as an important biometric modality after fingerprint and face. The accuracy and speed of iris-based systems currently deployed is promising and may be feasible in large-scale de-duplication systems.

Finally, it is possible to combine multiple biometric modalities including multiple fingerprints to increase overall de-duplication accuracy.

Recommendations

Based on the above deliberations, the Committee makes the following principal recommendations:

1. The Committee expects that the UIDAI could achieve at least 95% de-duplication accuracy using moderately good fingerprint images for a database size of 1 billion. Empirical image quality data of Indian ground conditions clearly show that such accuracy is achievable. In the global context, a de-duplication accuracy of 99% has been demonstrated to be achievable using good quality fingerprints against a database of up to fifty million.
2. In order to capture moderately good fingerprint images, a few simple but critical techniques during enrolment should be consistently followed, failing which material reduction in accuracy would occur. Manual and automated monitoring should be utilized to ensure consistent use of good enrolment practices.
3. In view of the above, the Committee feels that the UIDAI should collect photograph and ten fingerprints as per ISO standards described in Sections 8, 9 and 10.
4. Biometrics data are national assets and must be preserved in their original quality. In other words, quality must not be compromised through lossy image compression during storage or transmission.
5. While 10 finger biometric and photographs can ensure de-duplication accuracy higher than 95% depending upon quality of data collection, there may be a need to improve the accuracy and also create higher confidence level in the de-duplication process. Iris biometric technology, as explained above, is an additional emerging technology for which the Committee has defined standards. It is possible to improve de-duplication accuracy by incorporating iris. Accuracy as high as 99% for iris has been achieved using Western data. However, in the absence of empirical Indian data, it is not possible for the Committee to precisely predict the improvement in the accuracy of de-duplication due to the fusion of fingerprint and iris scores. The UIDAI can consider the use of a third biometric in iris, if they feel it is required for the Unique ID project.
6. A scheme must be designed to reward enrolling agencies for the capture of good quality images.

7. Specific best practices indicated in Section 12 should be observed in order to ensure interoperability, vendor independence, conformance to standards and improved performance.
8. The UIDAI along with other stakeholders should establish center(s) for on-going biometrics research, and provide reference implementation of enrolment process software designed for Indian conditions.

2 Introduction

The UID Authority of India (UIDAI) has been setup by the Govt. of India with a mandate to issue a unique identification number to every resident in the country. The UIDAI proposes that it create a platform to first collect the identity details of residents, and subsequently perform identity authentication services that can be used by government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identities in order to improve the efficacy of the service delivery.

The UIDAI has selected the biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information can be used to carry out de-duplication. Consequently, for government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that biometric information capture and transmission are standardized across all partners and users of the UID system.

The Government of India has in the past set up a number of expert committees to establish standards for various e-governance applications in the areas of Biometrics, Personal Identification and location codification standards. These committees have worked out standards in their respective categories, which may be uniformly applied for various e-governance standards.

As the UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications. It may also be necessary to enhance or clarify these standards,, and frame the methodology for the implementation of biometrics to ensure that they serve the specific requirements of the Authority.

3 Objective

The UIDAI biometrics committee ("the Committee") was constituted to provide the UIDAI with direction on the biometrics standards, suggest best practices and recommend biometric modalities for the UID system (Annexure I).

The objective of these biometrics specifications is to ensure consistent good quality biometric images and reliable interoperability across biometric capture devices, capture software and UID service delivery.

The success of the Unique ID is solely based on its ability to detect and eliminate duplicate identities during the enrolment process. The primary method for detecting duplicates will be through the comparison of the biometric feature set, which requires consistent, high quality images. A good biometric implementation design that ensures consistent quality from a variety of biometric capture devices is therefore, essential.

The biometrics will be captured for authentication by government departments and commercial organizations at the time of service delivery. They will invariably use capture devices and biometric software vendors different from the devices and software used by UIDAI. Consequently, biometric standards are essential to ensure reliable interoperability at reasonable cost during the authentication phase.

The purpose of this document is to identify applicable standards and recommend best practices to the UIDAI to achieve its objective.

4 Scope

- To develop biometric standards that will ensure the interoperability of devices, systems and processes used by various agencies that communicate with the UID system.
- To review the existing standards and, if required, modify/extend/enhance them so as to serve the specific requirements of the UIDAI.
- To specify design parameters of the standards that will be used for the UID system.
- To estimate the accuracy achievable using different biometric modalities in the Indian environment.
- To make recommendations to the UIDAI on the use of biometric modalities.

From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.

250

5 Target Audience

Any person or organization involved in designing, testing or implementing UID or UID compatible systems for the central government, state government or commercial organizations.

Any vendors and integrators of biometric devices and software targeting UID system compatibility.

6 Normative Reference

The following reference documents are indispensable for the application of this document.

IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint Image Compression Specification 1997

ISO/IEC 15444 (all parts), Information technology – JPEG 2000 image coding system

ISO/IEC 19785-1:2006. Common biometric exchange formats framework – Part 1: Data elements specifications

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

ISO/IEC CD 19794-6.3. Biometric data interchange formats – Part 6: Iris Image data working group draft

MTR 04B0000022. (Mitre Technical Report), Margaret Lepley, Profile for 1000 Fingerprint compression, Version 1.1, April 2004. Available at http://www.mitre.org/work/tech_papers/tech_papers_04/lepley_fingerprint/lepley_fingerprint.pdf

252

7 Standards

In the current IT world, as interoperability between devices and IT systems becomes a growing concern, the question is not whether to use standards but which standards to use. ANSI, INCITS, CEN, Oasis and ISO are just a few of the prominent agencies with published biometrics standards. After reviewing the charter of each body and current state of biometrics in India, the Committee selected the ISO standard. Within the ISO body of biometrics standards, the Committee will use data format standards. These standards are widely supported by vendors, and are used extensively. ISO data format standards also contain the maximum empirical information on usage, interoperability and conformance.

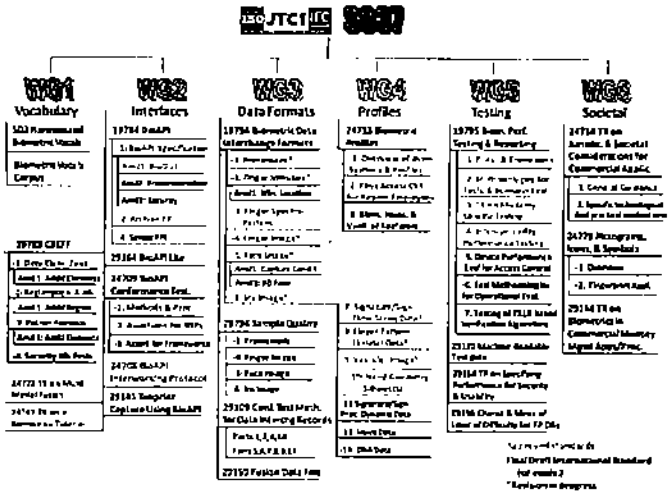


Figure 1 ISO Biometrics Standards Activity

8 Tailoring of Face Image Standards

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-5 Face Image Data Standard as the Indian Standard and will specify certain implementation values (tailoring) and best practices.

8.1 Section 7 Digital/Photographic requirements

The UIDAI will require face images for human visual inspection and duplicate check on a small subset. Visual inspection and automatic matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured.

8.1.1 For Enrollment and Authentication

Defining the values for face image standards as shown in Section 7.2, table 2.

Face Image Type Code	Scan resolution (dpi)	Color Space Code	Source Type Code	Inter-eye distance (pixels)	Facial Expression Code
Full Frontal (0x01)	300	24 bit RGB (0x01)	0x02 0x06	120	0x01

8.1.2 Source Type

Static face images (Code 0x02) from a digital still-image camera are strongly recommended. Single video frames from a digital video camera (Code 0x06) are also acceptable.

16.1.3 Expression

Face images should have neutral expression (non-smiling) with both eyes open and mouth closed.

16.1.4 Pose

Roll, pitch and yaw angle should not be more than $\pm 5^0$ (Figure 4 of ISO 19794-5).

8.2 Section 7 Image Compression Algorithm

8.2.1 . For Enrolment

For enrolment, uncompressed images are strongly recommended. Lossless JPEG 2000 color compression will be accepted for legacy purposes only.

16.2.2 For Authentication

Code 0x01 - JPEG 2000 compression is recommended. Maximum compression ration is 10.

8.3 Face Record Format

8.3.1 CBEFF Header

The UIDAI will not use information defined in Section 5.3 of ISO document.

8.3.2 Facial Record Header

The UIDAI will maintain single facial image.

8.3.3 Facial Information Block

The UIDAI will not use information defined in Sections 5.5.1 to 5.5.6 of ISO document.

8.3.4 Feature Point Block

The UIDAI will not use geometric feature points defined in Section 5.6 of ISO document.

9 Tailoring of Fingerprint Image Standard

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-4 Fingerprint Image Data Standard as Indian Standard and specify certain implementation values (tailoring) and best practices.

9.1 Section 7: Image Acquisition Requirements

The duplicate check during the enrolment phase will use 1:N matching. 1:N matching for large gallery size and high enrolment rate will require substantial computing resources. The matching time and matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured. It is also required that all ten fingers are captured whenever physically possible.

The goal during authentication is to achieve fast overall response while permitting a wide variety of capture devices and associated software. It is sufficient to capture only one or two fingers for reliable 1:1 authentication. The image quality needs for authentication are not as stringent as in enrolment.

9.1.1 For Enrolment

Setting level 31 or higher as shown in Section 7.1, table 1

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
31	197	500	8	200	EFTS/F

9.1.2 For Authentication

Setting level 28 or higher as shown in Section 7.1, table 2

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
28[1]	118	300	4	12	UID
30	197	500	8	80	None

9.2 Section 8 Finger Image record Format

9.2.1 Section 8.2.14 Image compression algorithm

9.2.1.1 Enrolment

Code 0 and 1 are strongly recommended. For legacy purposes only, lossless compression of code 2, 4 and 5 will be accepted.

9.2.1.2 Authentication

Code 4, compressed – JPEG 2000 is recommended. Code 0, 1, 2 and 5 are also acceptable. Code 3 must not be used. Maximum compression ration is 15.

[1] Level 28 is not specified in FBI's Electronic Fingerprint Transmission Specifications, Appendix F (commonly referred to as EFTS/F). It has been created to accommodate certain class of new generation lower cost single finger capture devices.

256

9.2.2 Section 8.3.3 Finger/palm position

The valid values for finger/palm position are 0 through 10, 13 through 15.

9.2.3 Section 8.3.7 Impression type

For enrolment image, only code 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

9.2.4 Section 8.3.10 Finger/palm image data

The estimated optimal fingerprint image captured under aforementioned specification of this standard in bitmap is 7.5MB per subject.

10 Tailoring of Minutiae Format Standard

UID Minutiae Format Standard will adopt the ISO/IEC 19794-2 Minutiae Format Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices.

10.1 Section 7.4.1.3 Impression Type

For enrolment image, only code[2] 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

10.2 Section 7.5 Extended Data

While the extended data area allows for the inclusion of proprietary data within the minutiae format, this is not indented to allow for alternate representation of data that can be represented in open manner, as defined in ISO/IEC 19794-2. In particular, ridge count data, core and delta data or zonal quality information shall not be represented in proprietary manner to the exclusion of publicly defined data formats.

The UID authentication process will not utilize extended data area for verification.

[2] Codes specified in ISO/IEC 19794-4, Section 8.3.7 are newer and superset of this table. Hence the reference is made to ISO/IEC 19794-4 Table 7.

11 Tailoring of Iris Standards

UID Iris Image Standard will adopt the ISO/IEC 19794-6 Iris Image Data Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices. The current (2005) version is under revision. A new version (2010) is expected to clear the ISO/IEC JTC 1/SC 37 sub-committee in January 2010. Therefore all references below are to the latest (November 2009) draft of the proposed standard. The Committee will revise this section after the ISO standard is published.

11.1 Section 7.4.2.2 Kind

Allowable values are KIND-VGA (2) and KIND_CROPPED (3) in Table 5.

11.2 Section 7.4.2.4 Image data

Every effort must be made by the vendor to register Capture Device Vendor ID and Capture Device Type ID with the appropriate registration authority. It is strongly recommended that these fields as described in Table 6 not be filled with zero value.

It is strongly recommended that quality information consisting of Quality score, Quality algorithm vendor ID and Quality algorithm ID as described in Table 6, shall be provided.

12 Best Practices

Specific recommendations for each modality listed below are based on prevailing standards, best practices followed by international users and the ground reality in India.

12.1 Face

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture	R	Full frontal, 24 bit color
Digital/Photographic requirements	R, S	Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2. Inter-eye distance – minimum 120 pixels.
Pose	S	Per ISO 19794-5 Section 7.2.2
Expression	R, S	Neutral expression. Specified as best practices.
Illumination	S	Per ISO 19794-5 Section 7.2.7
Eye Glasses	S	Per ISO 19794-5 Section 7.2.11
Accessories	R	Permissible for medical and ethical reasons only.
Multiple samples of face	M	Yes. Recommended for automatic face recognition.
Operational	S	Per ISO 19794-5 Section 7.2.4 - 7.2.10
Assistance	R	Yes. Specified as best practices.
Segmentation and feature extraction	M	Recommended for automatic face recognition
Quality check	R	Yes. Specified as best practice.
Storage & compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted.
Authentication		
Image capture	R	Same as enrollment
Compression	S	JPEG 2000 color compression recommended. Compression ratio to be less than 10:1.
Number of Images	R	One full frontal image

Figure 2 Face image

260

12.2 Fingerprint

Key Decisions	Decision Type[3]	Summary of Decisions
Enrolment		
Image capture		
Plain or rolled	R	Plain, live scan
Number of fingers	R	Ten
Device characteristics	S	Setting level 31 or above, EFTS/F certified
Quality check	R	Yes – specified as best practice
Operational		
Assistance	R	Yes – Specified as best practice
Corrective measure	R	Yes – Specified as best practice
Storage & transmission		
Compression	S	Uncompressed images strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.
Storage format	S	Per ISO Section 8.3. No deviation necessary
Minutiae format	S	Per ISO 19794-2. No deviation necessary.
Multi-finger fusion algorithm	R	Recommended. Application dependent.
Authentication		
Image capture		
Number of fingers	R	No minimum, no maximum. Application dependent. Recommended as best practice
Any finger option	M	Yes. Recommended as best practice
Retry	R	Maximum 5. Recommended as best practice.
Device characteristics	S	Setting level 28 or above
Transmission format	S	Per ISO. No tailoring necessary
Compression	S	JPEG 2000 compression recommended. Compression ratio to be less than 15:1
Minutiae format	S	Per ISO 19794-2. No tailoring necessary

Figure 3 Fingerprint

[3] R: Recommendation based on best practice/empirical data, S: Standard based, M: Management judgment.

12.3 Iris

Decision		Decision Type	Summary of Decision
Enrolment			
	Image	R	Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter
	Device Characteristics	R	Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control
	Operational	M	Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, indoor.
	Segmentation	R	Non-linear segmentation algorithm
	Quality Assessment	R	Per IREX II recommendations[4]
	Compression & Storage	S	ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).
Authentication		R, S	Same as enrollment except One or two eyes JPEG 2000 KIND_CROPPED of Table A.1

Figure 4 Iris

12.4 Biometrics Accuracy

The UIDAI's charter of assuring uniqueness across a population of 1.2 billion people mandates the biometrics goal of minimizing the False Accept Rate (FAR) within technological and economical constraints.

All published empirical data is reported using Western populations and database sizes of tens of millions. An accuracy rate (i.e., True Acceptance Rate) of 99% is reported in the test of commercial system performance[23]. Two factors however raise uncertainty on the extent of accuracy achievable through fingerprints: First, the scaling of database size from fifty million to a billion has not been adequately analyzed. Second, the fingerprint quality, the most important variable for determining accuracy, has not been studied in depth in the Indian context.

[4] IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. We anticipate similar outcome from IREX II. IREX II will be normative annexure to ISO 19794-6 (2010).

A technical sub-group was formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all were from rural regions, collected by different agencies using different capture devices and through different operational processes. Analysis reported in Annexure showed the UIDAI could obtain as good fingerprint quality as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

Based on rather extensive empirical results compiled by NIST and a first cut of Indian data analyzed in a short period, the following broad categorization can be made

1. The UIDAI can obtain fingerprint quality as good as that seen in developed countries. There is good evidence to suggest that fingerprint data from rural India may be as good as elsewhere when proper operational procedures are followed and good quality devices are used. There is also data to suggest that quality drops precipitously if attention is not given to operational processes.
2. It is possible to closely predict the expected fingerprint recognition performance. In the experiments, at 95% confidence, the sample database of a rural region is expected to achieve similar accuracy as Western data. By extrapolating NIST analysis of Western data, it is possible to conclude that fingerprint alone is sufficient to achieve minimum accuracy level of 95%, with moderately good fingerprints images.
3. Face is an invaluable biometric for manual verification. Its potential to contribute materially to improved FAR rate is however, limited particularly because of extremely large database size and high value of target accuracy.
4. Iris can provide accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy.

Empirical data has highlighted several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts.

- Simple operational quality assurance. A few simple operational techniques such as keeping a wet towel or maintaining the device in good working order can be superior to squeezing an additional fraction of a percent in accuracy rates through technical improvements. An unchecked operational process can increase the false acceptance rate to over 10%.
- In the data analyzed, 2% to 5% of subjects did not have biometric records. Missing biometrics is a license to commit fraud. It is believed that the failure is due to poorly designed processes. The enrolment process when examined, had loopholes which prevented it from detecting such omissions.
- The biometric software needs to be tuned to local data. Un-tuned software can generate additional errors in the range of 2 to 3%.

13 Members

13.1 Biometrics Committee

	Name, Affiliation
1.	Dr. B. K. Gairola, DG NIC - Chairman
2.	Dr. C. Chandramauli – Registrar General of India (RGI) – Member
3.	Dr. D. S. Gangwar, Joint Secretary, Rural Development- Member
4.	Dr. A. M. Pedgaonkar, RBI – Member
5.	Mr. Pravir Vohra, ICICI – Member
6.	Prof. Deepak Phatak, IIT Bombay – Member
7.	Prof. Phalguni Gupta, IIT Kanpur – Member
8.	Mr. R. S. Sharma, DG UIDAI – Member/Convener
9.	Mr. Rajesh Mashruwala, UIDAI – Member
10.	Mr. Srikanth Nadhamuni, UIDAI – Member

13.2 Face Sub-committee

1.	Dr. Richa Singh
2.	Dr. Mayank Vatsa
3.	Mr. Rajesh Mashruwala

13.3 Fingerprint Sub-committee

1.	Prof. Phalguni Gupta
2.	Dr. A. M. Pedgaonkar
3.	Mr. Rajesh Mashruwala
4.	Dr. Mayank Vatsa

13.4 Iris Sub-committee

1.	Prof. Phalguni Gupta
2.	Dr. Mayank Vatsa
3.	Mr. Rajesh Mashruwala

264

Annexure I
Notification of UIDAI constituting the Committee

No.45/DG-UIDAI/2009
Government of India
Planning Commission
Unique Identification Authority of India

R No.321, Yojana Bhavan
New Delhi – 110 001

Dated : September 29, 2009

OFFICE MEMORANDUM

The UID Authority of India has been setup by the Govt. of India with a mandate to issue a unique identification number to all the residents in the country. The main objective is to improve benefits service delivery, especially to the poor and marginalised sections of the society. To deliver its mandate, the UID Authority proposes to create a platform to first collect the identity details and then to perform authentication that can be used by several govt. and private service providers. A key requirement of the UID system is to minimize/eliminate duplicate UIDs in order to improve the efficacy of the service delivery. A possible way to ensure uniqueness of IDs (so that one resident gets only one ID) is to use biometric technologies. In order to ensure that an individual is uniquely identified and authenticated in an easy and cost-effective manner, it is necessary to ensure that the biometric information which is captured is capable of carrying out the de-duplication at the time of collection of information. Further, in order to achieve interoperability it is important that the capture and use of biometric information is standardized across all the partners and users of the UID system.

The Government of India, in the past, had set up a number of expert committees for standards to be used for various e-governance applications in arena of Biometrics, Personal Identification and location Codification Standards. These committees have worked out few standards in the respective categories to be uniformly applied for various e-governance standards.

As UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications, modify/extend/enhance them to ensure that they serve the specific requirements of UIDAI and frame the methodology for its implementation.

In view of the above, a Committee for framing the Biometric Standards for UIDAI is being setup to review the existing standards and modify/extend/enhance them so as to achieve the goals and purpose of UIDAI for de-duplications and authentication.

1. Charter of the Biometric Standards Committee

- To develop biometric standards that will ensure interopernbility of devices, systems and processes used by various agencies that use the UID system.
- To review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.

2. Composition of the Biometric Standards Committee

Following will be the composition of the Biometric Standards Committee:

1. Dr. BK Gairola, Director General, National Informatics Centre – Chairman
2. Dr. C. Chandramauli – Registrar General of India - Member
3. Dr. DS Gangwar, Jt Secretary, Min of Rural Development - Member
4. Dr. AM Padgaonkar, Reserve Bank of India – Member
5. Mr. Pravir Vora, ICICI - Member
6. Dr. Deepak Phatak, IIT Bombay - Member
7. Dr. Phalguni Gupta, IIT Kanpur – Member
8. Two Representatives from Technology Team of UIDAI – Members
9. Director General, UIDAI or his Nominee – Member/Convenor

Unique Identification Authority of India (UIDAI) will service this Committee.

The Committee will be able to invite representatives from user organisations and other Technology Experts as Special Invitees to solicit their views and advice on various aspects on the issue.

3. Technical Committee and Working Groups

The committee can also set up sub-committees that focus on various aspects of biometric standards such as fingerprints, Iris and facial image and working groups for conducting/developing reference implementations/proof-of-concept (POC) studies, specific research, field testing etc. on an as-needed basis. The Committee may meet from time to time and draft the standard document based on the feedback of sub committees and working groups and submit recommendations. The Committee may also set its own review process before recommending the final standards.

Working Groups can be created to assist the above committees by conducting proof-of-concept (POC) studies, specific research, field testing etc.

4. Review process

It is important that the standards remain unbiased, pragmatic, vendor neutral, interoperable, and cost effective. In biometrics where technology continues to progress rapidly, three parties - vendors, academia and enterprise users - have great deal of knowledge of the technology. The Committee's review process will leverage their knowledge without compromising on its charter.

The technical committee will publish a draft version of the document and solicit structured feedback from the members of the committee, technology vendors, academia and enterprise users. Such review process will also provide sufficient advance notice to the vendors to begin upgrade to their solution, thus reducing lead time between the final standards adoption and conforming solutions.

The feedback from the various groups will be reviewed by the technical committee and suitable changes made in order to incorporate useful inputs. The final draft will be sent over for a final review and then the ratified version of the standards will be released.

5. Deliverables of the committee

- Obtain consensus from Government stakeholders to adopt and use a common set of standards for interoperability, containment of biometrics system cost and wide spread propagation of Biometrics in governmental and private sectors.
- Review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.
- Ratify Biometrics standards from applicable base Indian and International standards, which meet needs of the UIDAI.
- Recommendation to UIDAI users to assure Interoperability of biometrics data
- Develop certification criteria for conformity, interoperability and performance.
- Maintain & Publish registry of recommended biometrics standards, interoperability recommendations and certification criteria.

6. Time-Frame

Keeping in view the commitment of UIDAI to start issuing UIDs within twelve to eighteen months, it is necessary that the Committee presents its report on standards as early as possible. Hence the Committee will present its Final Report to the undersigned on Biometric Standards to be adopted by UIDAI within 90 days of its constitution.

7. Miscellaneous

The non-official members of the Committee and Special Invitees will be reimbursed the cost of their travel and other incidental expenses as per Rules as and when they travel to attend the Committee meetings.

29.9.09

(R S Sharma)
Director General & Mission Director

Copy forwarded to the Chairman and Members of the Committee for information and necessary action.

Copy to: Cabinet Secretary/ Principal Secretary to the PM/All Secretaries to Govt. of India/All Chief Secretaries of the States/UTs for information.

269

Annexure II Technical Data

Biometrics Basics

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person. The relevance of biometrics in modern society has been reinforced by the demand for large-scale identity management systems whose functionality relies on accurately determining an individual's identity. No single biometric is expected to effectively meet all the requirements imposed by all applications. In other words, no biometric is ideal, but a number of them are admissible[1].

Demographic data is used along with the biometric information to improve the de-duplication process. For example, when a duplicate is suspected, a manual review of all available information of the person will also include a review of the demographic data.

Face

Photos of the face are commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. The face biometric can work with legacy photographs, videotapes and other image sources.

A face needs to be well lighted using controlled light sources for automated face authentication systems to work well. There are many other such technical challenges associated with robust face recognition. Face is currently a poor biometric for use in de-duplication. It performs better in verification but not at the accuracy rates that are sometimes claimed. An obvious way for an undesirable person to avoid face identification is by the use of disguise, which will cause False Negatives in a screening application. In general, it is a good biometric identifier for small-scale verification applications.

Fingerprint

There is a long tradition in the use of fingerprints for identification. Fingerprints are easily sampled with low-cost fingerprint scanners. They can also be sampled by traditional low-tech means and then cheaply and easily converted into digital images. Fingerprints also lend themselves very well to forensic investigation.

There is a large variation in the quality of fingerprints within the population. The appearance of a person's fingerprint depends on age, dirt, and cuts and worn fingers, i.e., on the occupation and lifestyle of the person in general. Sampling of the fingerprint is through contact, i.e., pressing the finger against the platen of a fingerprint reader. As a result, there can be technical problems because of the contact nature of acquisition and problems related to the cleanliness of the finger and the platen. Additionally, there are people who may not have one or more fingers [5].

Fingerprint technology constitutes approximately half of the total biometrics market[5].

Iris

The iris is the annular region of the eye, bounded by the pupil and sclera on either side. Iris is widely believed to be the most accurate biometric, especially when it comes to False Accept Rates. Therefore, the iris would be a good biometric for pure de-

[5] IDC & Acuity Market Research Reports.

duplication applications. The iris sample acquisition is done without physical contact and without too much inconvenience to the person whose iris image is being acquired. Iris has no association with law enforcement and has not received negative press and may therefore be more readily accepted.

There are few legacy databases and not much legacy infrastructure for collection of the iris biometric. Large-scale deployment is consequently impeded by the lack of an installed base. This will make the upfront investment much higher. Since the iris is small, sampling the iris pattern requires a lot of user cooperation or the use of complex and expensive devices. The performance of iris authentication can be impaired by the use of spectacles or contact lenses. Also, some people may be missing one or both eyes while others may not have the motor control necessary to reliably enroll in an iris based system.

Until recently, iris code representation and matching was proprietary and patented. Iris is emerging as the third standard biometric identifier after expiration of patents and changes in vendor practices.

The gross false accept and false reject error rates associated with the fingerprint, face and iris modalities reported in literature are shown in Figure 5 [2].

Biometric identifier	**Reference**	**FRR**	**FAR**
Fingerprint	NIST FpVTE	0.1%	1%
Face	NIST FRVT	10%	1%
Voice	NIST 2004	5-10%	2-5%
Iris	ITIRT	0.99%	0.94%

Figure 5 FAR and FRR error rates

272

Face Image Best Practices

Summary

Face images will be used primarily for human visual inspection. However, automatic face recognition may be used as the secondary means of authentication/de-duplication. Figure 6 summarizes key decisions for face images.

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture	R	Full frontal, 24 bit color Inter-eye distance – minimum 120 pixels.
Digital/Photographic requirements	R, S	Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2.
Pose	S	Per ISO 19794-5 Section 7.2.2
Expression	R, S	Neutral expression. Specified as best practices.
Illumination	S	Per ISO 19794-5 Section 7.2.7
Eye Glasses	S	Per ISO 19794-5 Section 7.2.11
Accessories	R	Permissible for medical and ethical reasons only.
Multiple samples of face	M	Yes. Recommended for automatic face recognition.
Operational	S	Per ISO 19794-5 Section 7.2.4 - 7.2.10
Assistance	R	Yes. Specified as best practices.
Segmentation and feature extraction	M	Recommended for automatic face recognition
Quality check	R	Yes. Specified as best practice.
Storage & compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted.
Authentication		
Image capture	R	Same as enrollment
Compression	S	JPEG 2000 color compression recommended. Compression ratio to be less than 10:1.
Number of Images	R	One full frontal image

Figure 6 Face

Enrolment

Face image capture

Full frontal face image provides sufficient information for both human visual inspection (by operator) and automatic face recognition algorithms. In order to obtain a good quality image, 24-bit color image with minimum 90 pixels of inter-eye distance is required. The Committee recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region. In special circumstances, assistance may also be provided but in no case should the face or body part (hand, arms) of the assisting person or any object appear in the photograph.

Digital/Photographic requirements

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with enrollee demographic data at the point of capture, thus reducing possible errors. In villages where power source may be difficult to obtain, it is simpler to supply power from the computer.

For capturing face image, it is simpler for the operator to adjust the camera instead of the enrollee to position himself/herself at the right distance or in the right posture. The capture device should use auto focus and auto-capture functions. The output image should not suffer from motion blur, over or under exposure, unnatural colored lighting, and radial distortion. Interlaced video frames are not allowed.

Pose

Face image should be full frontal with 0^0 of yaw, pitch and roll angles. However, in operational conditions, variation of $\pm 5^0$ is permissible.

Expression

Expression strongly affects the performance of automatic face recognition and also affects accurate visual inspection by humans. It is strongly recommended that the face should be captured with neutral (non-smiling) expression, teeth closed and both eyes open.

Illumination

Poor illumination has high impact on the performance of face recognition. It is difficult for human operators as well to analyze and recognize face images with poor illumination. Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots.

Eye Glasses

Face images with and without eyeglasses may have an impact on face recognition. The impact is greater if the glasses automatically tint under illumination. If the person normally wears glasses, it is recommended that the photograph be taken with glasses. However, the glasses should be clear and transparent so that pupils and iris are visible. If the glasses are with tint, then direct and background lighting sources should be tuned accordingly.

Accessories

Use of accessories that cover any region of the face is strongly discouraged. However, accessories like eye patches are allowed due to medical reasons. Further, accessories like turban are also allowed due to ethical reasons.

Multiple samples of face

For visual inspection by humans, the single face image of a person is sufficient. However, for de-duplication and authentication of individuals who do not have fingerprints, automatic face recognition is recommended. To perform accurate authentication in such cases, capture of multiple face images is strongly recommended during enrolment. There should be three samples, out of which one should be frontal image with yaw, pitch and roll angle as 0^0. The other two images should be left and right semi profile with yaw as $\pm 20^0$ to $\pm 30^0$, and the roll and pitch should be 0^0.

Operational
Similar to fingerprints, the single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, operator training and assistance are important for yielding good quality images. Operators will be trained to obtain the best possible face images that satisfy requirements.

Segmentation and feature extraction
Segmentation and feature extraction are only required for automatic face recognition algorithms. The algorithms for both remain proprietary.

Quality check
Image quality is one of the most important factors for both human inspection and automatic face recognition algorithms. The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image and image is stored only if it meets a certain quality threshold.

Storage and Compression
According to Figures 12 and 13 of ISO face image standards, the performance of face recognition algorithms reduce significantly if the compression factor is greater than 10. Further, as mentioned previously, these are our national assets and should be captured and stored for long-term use. For preserving the quality of image, it is strongly recommended that uncompressed images should be stored in the database.

Authentication
The authentication process consists of steps similar to enrolment.

Image Capture
Image capture for 1:1 verification should also follow standards for enrolment as defined earlier in this Section.

Compression
For verification, images with JPEG 2000 compression ration of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

Number of Images
For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

275

Fingerprint Best Practices

Summary

Figure 7 summarizes the key parameters for fingerprint. The Committee further classifies the decision into

1. Standards based (S): Do ISO or other standard bodies directly provide available choices?
2. Recommendation based (R): Are there studies that provide sufficient evidence for us to make an informed decision?
3. Management judgment (M): Management decision based on project context.

The remaining section has a brief explanation of each decision.

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture		
Plain or rolled	R	Plain, live scan
Number of fingers	R	Ten
Device characteristics	S	Setting level 31 or above, EFTS/F certified
Quality check	R	Yes – specified as best practice. Avoid NFIQ quality 4 and 5 level fingerprints.
Operational		
Assistance	R	Yes – Specified as best practice
Corrective measure	R	Yes – Specified as best practice
Storage & transmission		
Compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.
Storage format	S	Per ISO Section 8.3. No deviation necessary
Minutiae format	S	Per ISO 19794-2. No deviation necessary.
Multi-finger fusion algorithm	R	Recommended. Application dependent.
Authentication		
Image capture		
Number of fingers	R	No minimum, no maximum. Application dependent. Recommended as best practice
Any finger option	M	Yes. Recommended as best practice
Retry	R	Maximum 5. Recommended as best practice.
Device characteristics	S	Setting level 28 or above
Transmission format	S	Per ISO. No tailoring necessary
Compression	S	JPEG 2000 compression recommended. Compression ratio to be less than 15:1
Minutiae format	S	Per ISO 19794-2. No tailoring necessary

Figure 7 Fingerprint

Enrolment

The enrolment process can be broken down into image capture ("client") and de-duplication ("server") side components. The client side captures the image, performs local processing and storage. The server side receives the image, performs quality check and finally executes the computational intensive task of duplicate checking against the gallery.

Image capture

During image capture, the factors to consider are:

1. Type of image and number of fingers to capture
2. Device used for capturing the image
3. Immediate processing including segmentation of slap, sequencing of fingers, rotational correction and quality check of image
4. Storage when the images need to be stored

Plain or rolled

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger. The operation difficulty in capturing rolled image rules out its use in the UID system.

Number of fingers

In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image. Considering the fingerprint quality of rural workers, the Committee recommends capturing prints of all ten fingers, the maximum possible.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images[6]. The biometrics sample captured during enrolment needs to be the best sample possible. Therefore following best practices of leading countries, the Committee recommends the use of EFTS/F certified devices that operate at level 31 or above.

Capture & quality check

Once the image has been captured, one can perform basic quality check and image improvement. The enrollee must be asked to retry enrolling if the image quality is poor. The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 normally should not be used for enrolment purposes.

---

[6] It should be noted that two devices with identical scan resolution, pixel depth and dynamic range do not provide similar quality images. A number of laboratory tests have shown that a 500 dpi device from one vendor performs better than a 1000 dpi device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements.

Operational

The single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, the following have been shown to be critical factors:

1. Operator Assistance: Operators will be trained to guide the enrollee's hand and apply pressure if necessary to obtain best possible image quality.
2. Corrective measures & retries: If the initial capture is unsatisfactory, the operator will be trained to provide corrective measures such as wiping fingers with a wet cloth or applying lotion. Only after all such measures are exhausted in five attempts, will the operator be able to override the (forced capture) quality gate.

Storage and Transmission

Once the quality check is complete, the image needs to be retained. The data format of storage should be such that other applications can access the data.

Compression

Biometric data are national assets and should be captured and stored for long-term use. To preserve the quality, the Committee strongly recommends uncompressed images. Transmission of images may be made in JPEG 2000 or WSQ lossless compression for legacy or compatibility purposes. Any form of lossy compression is not accepted. In uncompressed mode, the total storage required for the entire population is 10,000 TB.

Storage format

ISO standard prescribed format is sufficient for our needs.

De-duplication minutiae format

The minutiae representation has been standardized. However, the standardization allows vendor proprietary data fields. The trade-off is between performance and accuracy through enhanced minutiae data versus higher level of vendor dependence. Based on the accuracy and performance trade-offs reported by NIST, it is acceptable to use the proprietary format of the extractor-matcher of the vendor selected for de-duplication.

Multi-finger fusion

Different algorithms are available to obtain consolidated score [7] and [28]. The selection of the algorithm will make material difference to the overall accuracy. ISO and other bodies do not make recommendations, nor do they provide empirical study. The UIDAI will conduct its own analysis to identify the best multi-finger fusion algorithm.

Authentication

The authentication process consists of steps similar to the enrolment process, but its requirements for accuracy, performance and interoperability are different. Since the authentication process is performing 1:1 verification, the captured image may be of lower quality compared to the image captured during the enrolment process.

Image capture

Number of fingers

It is obvious that a fewer number of fingers should be required for verification to achieve a satisfactory accuracy target. A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers.

Any finger option

The normal practice is to use one specific finger, say the index finger for verification. However, current technology could allow the person to scan any finger. This is not merely a question of convenience. Certain fingers, depending on the condition of the finger, will perform better in matching. While one cannot easily determine this a priori, any frequent user will learn it by experience. This improves subsequent user experience and could potentially improve match accuracy.

Retry

The decision on number of retries has different implications during authentication. In case of enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture". In case of authentication, the operator needs to find an alternate method of authentication if fingerprint verification fails. The operator/application would not know the cause of verification failure. The failure could be because the fingerprint did not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the system to declare "no match". A timeout will be implemented in service after five attempts.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. Higher resolution does not necessarily produce better images. Considering the UIDAI's goal of making authentication ubiquitous and the availability of low cost new technology devices, the Committee has defined a new standard for the scanner used in the authentication process. It is envisioned that the UIDAI will provide certification criteria for this standard.

Transmission format

The captured image needs to be sent to the UID server for matching in real time. Two factors will decide the format of the image to be sent. If the transmission bandwidth is low, it is prudent to send as little data as possible. On the other hand if the computing device associated with the capture device has very limited processing power, it is prudent to do minimal amount of local computation. In the first case, the transmission will contain extracted minutiae. In the second, it will contain the compressed raw image. For example, a capture device connected to a computer communicating over a mobile network could send minutiae by performing local extraction. A dedicated image capture device with built-in network connectivity is able to do little local processing and may send raw image.

The UID software will support raw image format, compressed image format as well as ISO standard minutiae format to be transmitted, in order to provide maximum flexibility during authentication. It is understood that raw or compressed image will give a higher level of accuracy.

Compression

If the raw image is to be sent, JPEG 2000 compression is recommended, WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed image will be accepted, it is not recommended. JPEG compression is not accepted. There is sufficient data to indicate that compression ratio of 15 does not affect verification accuracy. Compression is not relevant if minutiae data is to be sent for verification.

Minutiae format

As discussed in the previous section, the biometric sample being transmitted could be minutiae data or image. If the data is minutiae and the UID server has matcher that best pairs with the extractor used by the authenticating agency, it will use the proprietary data. If the server does not have matching matcher, it will only use "standard" minutiae data.

280

Iris Image Best Practices

Summary

Compared to fingerprinting, iris capture is less studied and less standardized. For example, fingerprint scanners are tested and certified per EFTS/F standard. No such equivalent iris device certification is available. It is necessary to provide greater number of parameter specifications to ensure quality iris capture.

Figure 8 summarizes key decisions for UIDAI iris design.

Decision		Decision Type	Summary of Decision
Enrolment			
	Image	R	Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter
	Device Characteristics	R	Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control
	Operational	M, R	Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, capture location: indoor.
	Quality Assessment	R	Per IREX II recommendations[7]
	Compression & Storage	S	ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).
Authentication		R, S	Same as enrollment except One and/or two eyes JPEG 2000 KIND_CROPPED of Table A.1

Figure 8 Iris

The remaining section has a brief explanation of each decision.

[7] IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. IREX II will be a normative annexure to ISO 19794-6 (2010).

Enrolment

Iris image

Capture of two eyes simultaneously provides several advantages[8]. Iris pattern of each eye is not correlated, giving two independent biometric feature sets. It assures correct assignment of left and right eyes and allows for more accurate estimation of roll angle.

In order to obtain good quality template, the iris image diameter should be minimum 140 native pixels. The Committee recommends 170 pixels for optimum quality.

In order to retain sufficient image surrounding of the iris for the purpose of identifying the left or right eye as well as for a more accurate iris segmentation, the margins around the iris portion of the image need to be at least 50% of the iris diameter on the left and right sides of the image, and a least 25% of the iris diameter on the top and bottom of the image.

Device Characteristics

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with the enrollee demographic data at the point of capture, thus reducing possible errors. In villages where a power source may be difficult to obtain, it is simpler to supply power from the computer.

Iris capture is a new experience for the public[34]. It is faster and simpler for the operator to adjust the camera instead of the enrollee positioning himself/herself at the right distance or in the right posture. It is recommended that the capture device should be more than 300 mm away from the enrollee to be considered non-intrusive. The capture device should use auto focus and auto-capture functions. In special circumstances where the enrollee has to position himself or herself, the capture device should be more than 100mm away but the device should use a visor or other mechanical alignment aid to enable the enrollee to position themselves.

In order to provide an acceptable level of usability and ease of alignment, the camera must allow for some variability in the position of the iris center relative to the camera. This variability is defined by position tolerances in the horizontal, vertical, and axial dimensions that together define a volume (the "capture volume") within which the center of the iris must be located in order to enable image capture. For two eye capture devices, the capture volume dimensions for devices without mechanical alignment aids are 19 mm wide, 14 mm high, and 20 mm deep, and for devices with such aids, 19 mm wide, 14 mm high, and 12 mm deep.

The ability of an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time is less than 33 ms, recommended being 15ms.

The iris image capture device must be capable of capturing light in the range of 700 to 900 nanometers. The camera's near infrared illuminator(s) must have a controlled spectral content, such that the overall spectral imaging sensitivity, including the sensor characteristics, transfers at least 35% of the power per any 100 nm-wide sub-band of the 700 to 900 nm range.

---

[8] Material derived from [32]

The iris image capture sensor shall use progressive scanning.

In order to achieve acceptable time-to-capture and FTA rates, the iris image sampling frequency must be at least 5 frames per second.

The capture devices typically provide infrared lighting using LEDs to illuminate the iris. The illumination is in a range partly visible to the human eye. Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1.

In order to achieve acceptable recognition accuracy, the iris acquisition sensor must achieve a signal-to-noise ration of at least 36dB.

Within the frequency range of interest, 700 to 900 nm, the iris sensor shall generate images with at least 8 bits per pixel.

Operational considerations

As mentioned earlier, it is strongly recommended that the operator and not the enrollee handle the capture device. The enrollee will be required to sit (or stand) in a fixed position, like taking a portrait photograph; the operator will adjust the camera.

The iris capture device or the connected computer shall be able to measure the iris image quality. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality.

The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off enrollee's eyes.

Segmentation and feature extraction

Segmentation and feature extraction remain proprietary. As reported in the IREX study, the vendor providing segmentation does not have to be the vendor providing matching algorithm. In fact, best of breed selection appear to be superior to any single-vendor solution.

Quality assessment

It has been noted that image quality is the single most important factor for match accuracy. IREX II study is underway to quantify and provide best practices recommendations on the image quality. The report, expected in April 2010, will become the normative annexure to ISO 19794-6 (2010). Therefore the Committee will defer detailed quality recommendations until publication of the standard.
One method widely used for ensuring good iris images is recommended here. An Iris camera takes streaming images. It is recommended that the device take successive 3 to 7 images and use local matching algorithm to match them against each other (after feature extraction). The image is considered to be of satisfactory quality if hamming distance of the match is below 0.1.

Compression and storage

The iris images, like fingerprints are considered to be national assets. They should be stored in ISO standard format using either JPEG 2000 or PNG lossless compression (KIND_VGA). It is expected that each enrollee will require 150 Kbytes of storage space, thus requiring total storage space of 200 Terabytes for the entire population.

Authentication

For 1:1 verification, any one eye will suffice, though application may require higher-level assurance whereby both eyes can be verified. Iris verification requires the image to be sent to the server for matching. It is recommended that the image be compressed to KIND_CROPPED_AND_MASKED or KIND_CROPPED using JPEG 2000. Resulting image size will between 2KB to 10 KB. Any of the larger formats specified by the ISO standard are acceptable, though not necessary.

Biometrics Accuracy

The consequences of FAR and FRR during authentication are central to the judicial design of the UID system. FAR determines potential number of duplicates, FRR determines number of enrolments necessitating manual check, hence labor cost. While trade-off between the two rates is certainly possible, there are upper bound requirements for each. Upper bound for each rate is set at 1%.

No empirical study is available to estimate the accuracy achievable for fingerprint under Indian conditions. Indian conditions are unique in two ways:

- Larger percentage of population is employed in manual labor, which normally produces poorer biometric samples.
- Biometric capture process in rural and mobile environment is less controllable compared to the environmental conditions in which Western data is collected.

To estimate achievable accuracy under Indian conditions, following methodology was employed:

1. Estimate achievable accuracy under Western conditions for a one billion sized database.
2. Estimate difference in image quality between Western and Indian conditions.
3. Using image quality, estimate change in achievable accuracy under Indian conditions.

There is no indication to believe that iris accuracy changes from one racial/geographical population to another. However, no definitive study is available.

Step 1: Estimating achievable accuracy

NIST reports FAR of 0.07% at FRR 4.4% for 6 million fingerprint gallery size using two plain fingers [21]. Similar results were reported for FBI's IAFIS System of 46M samples. It is safe to conclude that 99% accuracy (TAR) can be achieved for database size of 50 million.

	Thresholds 1300, 1880		Thresholds 1400, 2025		
Shape Filter	FAR	TAR	FAR	TAR	Matches per Second
Off	0.30%	96.3%	0.07%	95.6%	734K
On	0.32%	96.1%	0.07%	95.5%	1035K

Figure 9 Two-finger identification accuracy

Several NIST reports allow us to estimate the scaling of above data for larger gallery size and for ten fingers.

- False Acceptance Rate is linearly proportional to gallery size at constant TAR as shown in Figure 11.
- False Rejection Rate does not vary over gallery size as shown in Figure 12.
- Based on these findings, one can expect that on a database size that is 200 times larger (1.2 billion versus 6 million), the same system will have an FAR of

approximately 0.07*200 = 14%. The FRR can be expected to be about 4% based on matching of 2 finger plain fingerprints.

- Figure 10 lists effect on FAR by increasing the number of fingers for the same FRR [22].

Number of Fingers	FRR %	FAR %
2	10.3	29.2
10	10.9	0.0

Figure 10 Accuracy of multiple fingers

- Based on the above and reviewing underlying data, one can ballpark a 1,000 improvement in FAR between two-finger matching and ten-finger matching (all other things being equal). So the estimated FAR estimate of 14% should be expected to be 1,000 times less, that is, to 0.14% at FRR rate of 4%. Using further conversation factor of 10X change in FAR results in 2X change in FRR, this number is the equivalent of *FAR 1.4% at FRR rate of 2%*. In other words, NIST data indicates de-duplication accuracy (TAR) greater than 95% is achievable for ten-finger matching against a database size of one billion.

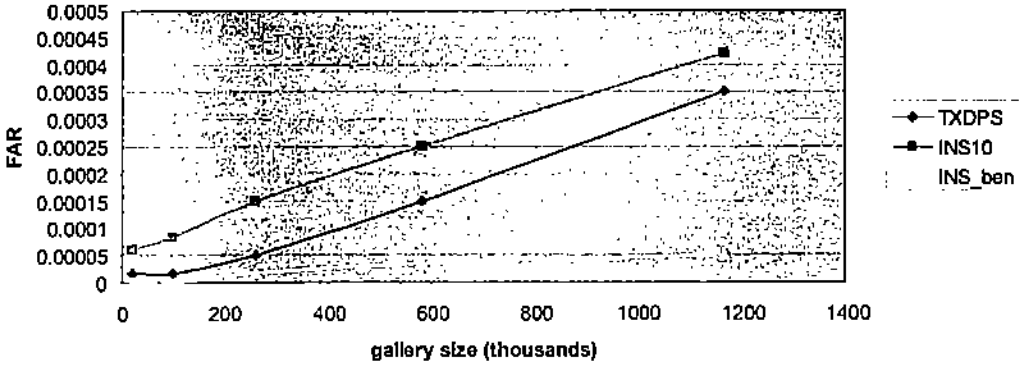


Figure 11 FAR as function of gallery size

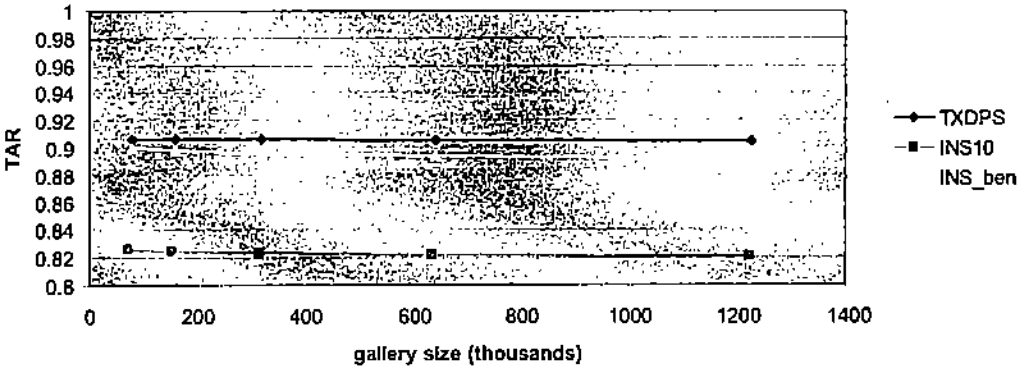


Figure 12 TAR as function of gallery size

Step 2: Image quality difference

It has been shown that match rates accuracy can be estimated from the fingerprint image quality score. NIST classifies scores into five bins. Western data accuracy rates for the bins are shown in Figure 13. Bins 1 and 2 are nearly identical, producing close to 99% true match in 1:1 verification. Bins 4 and 5 result in unacceptably low true match rates. Of particular note is bin 5, which could result in as low as 80% match rate (or 20% false accept rate).

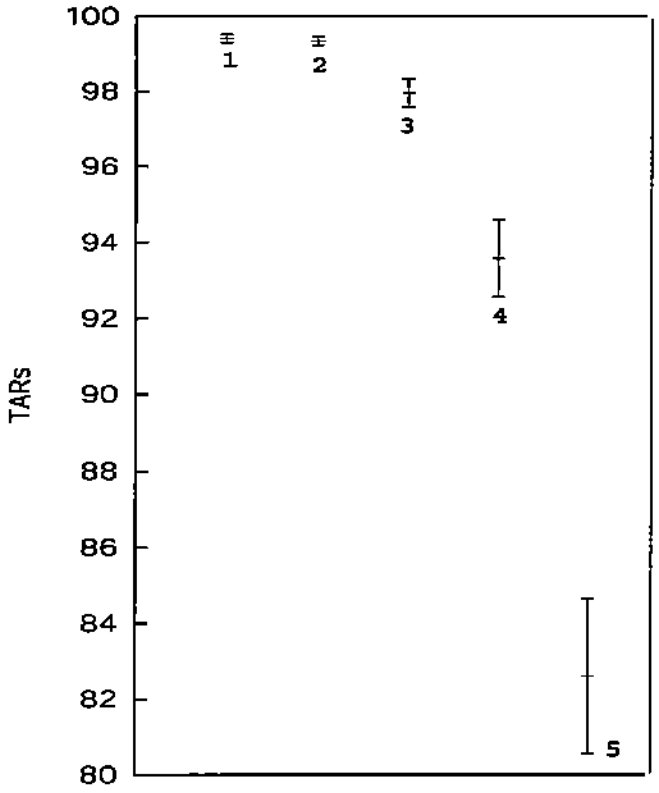


Figure 13 Accuracy Range by image quality

In a "typical" sample analyzed to arrive at the above rate[24], NIST has bin distribution shown in Figure 14 and Figure 15. Bins 4 and 5 in both datasets are less than 5% of the total sample.

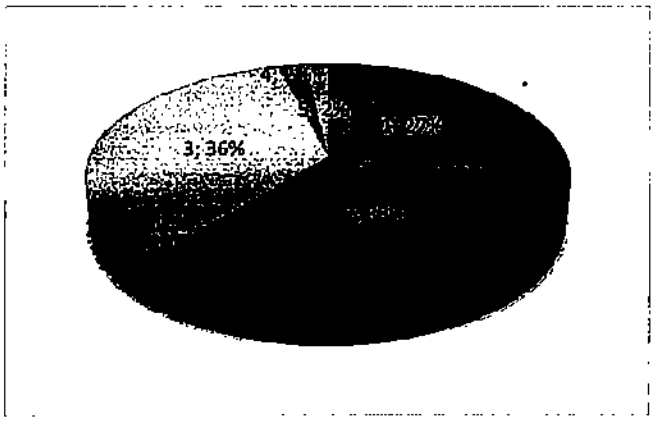


Figure 14 US-VISIT image quality distribution for right index finger

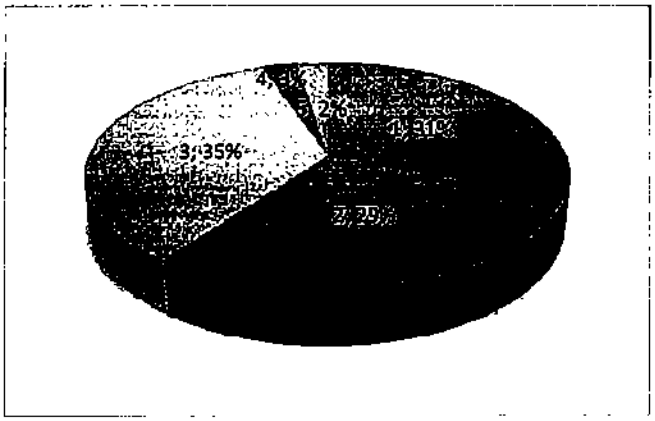


Figure 15 US-VISIT image quality distribution for left index finger

Indian Ground Conditions

The research team at IIIT Delhi focused on the ability to leverage image quality assessment tools in (1) analyzing the input biometric samples that are obtained from diverse, disparate sensors and (2) characterizing the samples based on the quality and amount of information present. Using three fingerprint databases, fingerprint image quality based experimental evaluation was performed.

1. DB1. This database contains images from 27 urban individuals (or 1350 images) and 81 rural individuals (or 1620 images). This database is prepared using single impression sensor meeting FIPS 201 APL and FBI Image Quality Specifications.
2. DB2. Images captured using slap scanner. This database contains slap images from over 20,000 individuals. Each slap fingerprint image was segmented using a commercial segmentation tool. After segmentation, the database contained 200K images. The four-finger slap sensor was EFTS/F certified and operated at level 31.
3. DB3. Pre-segmented rural slap database pertaining to about 5600 individuals (around 56,000 images). The four-finger slap sensor was EFTS/F certified and operated at level 31.

Using DB1, experimental test bed and statistical tests were prepared, followed by evaluation using DB2 and DB3. Using NIST provided Fingerprint Image Quality software (NFIQ), images were classified in to bins according to the image quality score. The bin

distributions for Indian databases are shown in Figure 16 through Figure 19. Of particular interest is significantly large bin 4 & 5 numbers for DB2 as well as DB1 rural sample. In contract, DB3, another rural area shows exceptionally high bins 1 and 2.

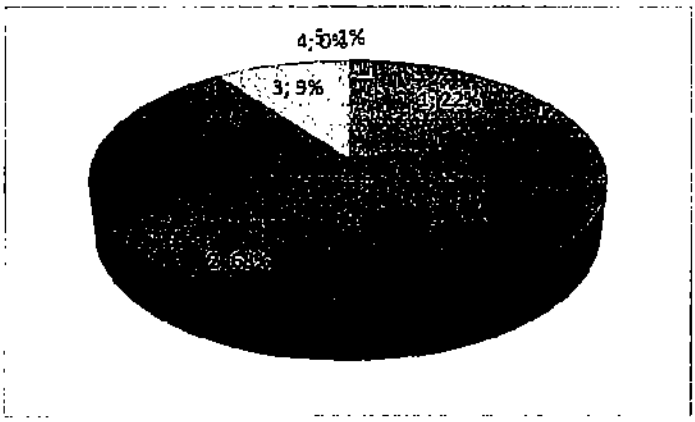


Figure 16 Image quality score distribution for DB1 Urban sample

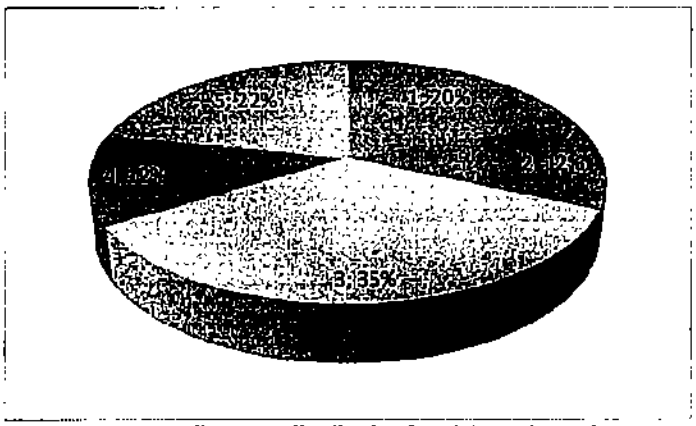


Figure 17 Image quality score distribution for DB1 Rural sample

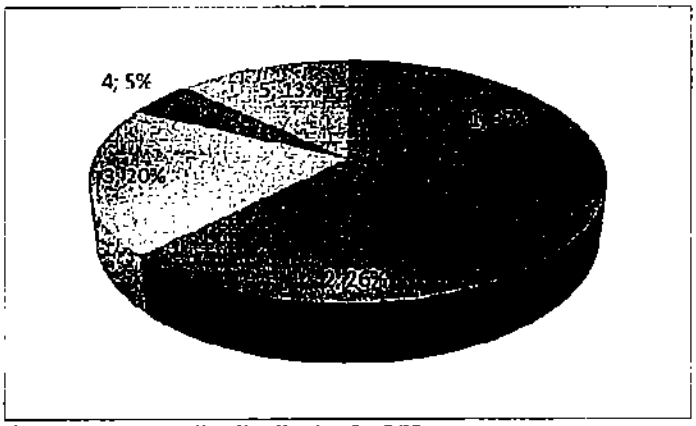


Figure 18 Image quality distribution for DB2

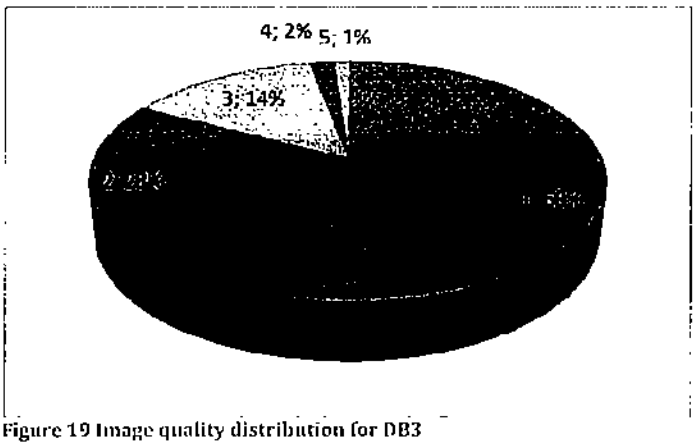


Figure 19 Image quality distribution for DB3

Step 3 Comparison & quality estimates

Since, DB2 and DB3 databases have only a single impression per finger, it is impossible to compute ROC or CMC plots and compute recognition accuracies. However, using existing Western results[24], it is possible to closely predict the expected fingerprint recognition performance.

Figure 20 and Figure 22 compare quality of left and right index finger respectively. Against x axis of accuracy (FAR), it shows cumulative bin score. Line over the Western curve (blue line) indicates that expected accuracy of the sample will be better than that of the Western population. Any points below the Western curve indicate that expected accuracy of that sample will be worse than the Western population.

DB3 shows quality superior to Western image quality while DB2 shows significantly inferior quality. While both samples are from two different rural areas of two different states, the expected accuracy is vastly different.

290

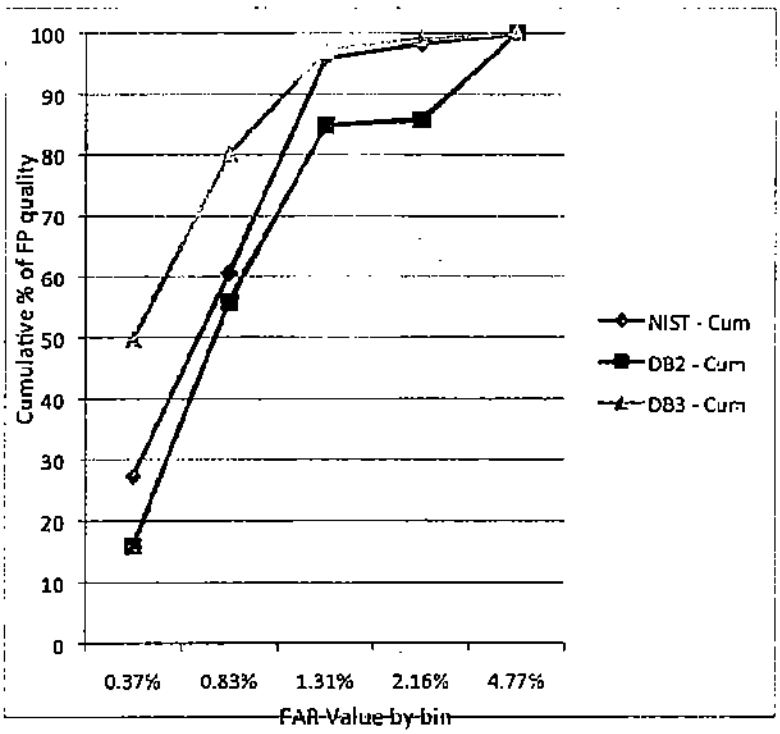


Figure 20 Right index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5
	0.37%	0.83%	1.31%	2.16%	4.77%
NIST	27.28	33.32	35.37	2.23	1.8
NIST - Cum	27.28	60.6	95.97	98.2	100
DB2	15.87	40.08	28.88	0.99	14.18
DB2 - Cum	15.87	55.95	84.83	85.82	100.00
DB3	49.73	30.51	16.97	2	0.79
DB3 - Cum	49.73	80.24	97.21	99.21	100.00

Figure 21 Right index finger numerical data

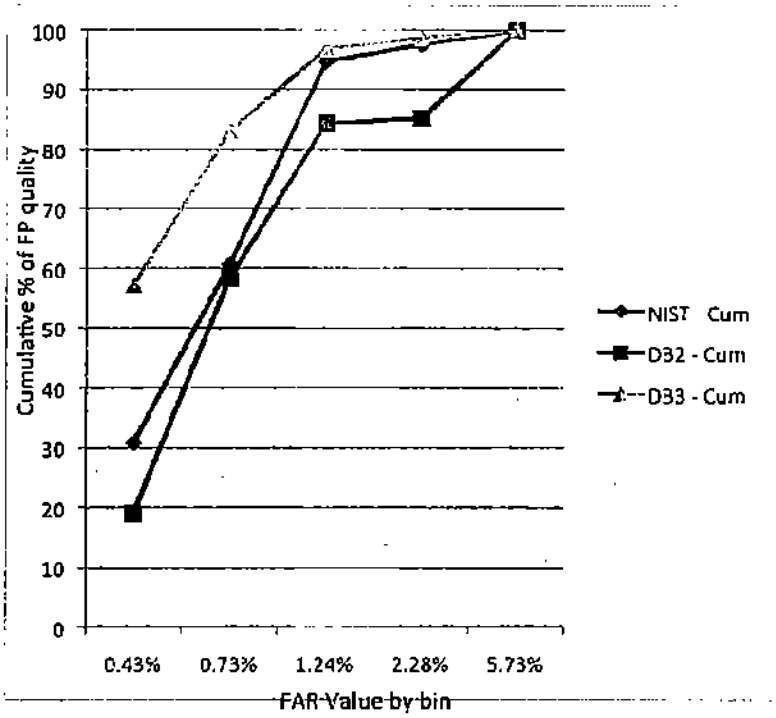


Figure 22 Left index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5
	0.43%	0.73%	1.24%	2.28%	5.73%
NIST	30.83	29.78	34.08	2.88	2.43
NIST - Cum	30.83	60.61	94.69	97.57	100
DB2	18.99	39.36	25.87	0.90	14.88
DB2 - Cum	18.99	58.35	84.22	85.12	100.00
DB3	57.25	25.77	13.8	1.87	1.31
DB3 - Cum	57.25	83.02	96.82	98.69	100.00

Figure 23 Left index finger comparison

Conclusions

NFIQ results on the databases seem to be encouraging especially if the fingerprint images are captured using good operational processes. For the majority of images, quality scores vary from excellent to good. Using these images, the typical performance of fingerprint feature extraction and matching should meet expectations. Therefore, to achieve good recognition accuracy, good quality images should be collected using optimized operational mechanisms and good sensors.

- The UIDAI can achieve fingerprint accuracy of a quality similar to developed countries. There is good evidence to suggest that Indian rural data may be as good as developed country settings when proper operational procedures are followed and good quality devices are used.
- It is possible to closely predict the expected fingerprint recognition performance. In the experiments, it is observed that, at 95% confidence, DB2 is expected to show lower accuracy compared to the Western data whereas DB3 is expected to achieve similar accuracy (for Q = 1, 2, and 3, 99% TAR with about 1% FAR).

- It is believed that DB3's improved image quality is due to better operational procedures. A few simple methods were used in DB3 data collection, such as:
  1. Using wet towels to remove dirt and moisten dry fingers
  2. Using minimum quality threshold to ensure that extra efforts are made to capture good prints from hard to obtain fingers and
  3. Keeping scanning devices in operational order

  These resulted in exceptionally good bin 1 and 2 distribution.
- It is also observed that the slap fingerprint segmentation tools require some prior training for Indian databases. After some training, segmentation results improve by 2-3%. This also suggests that in deploying a biometrics (fingerprint) system, a carefully designed a priori training set and procedure will help in improving performance.
- Since NFIQ tool is trained using Western data, there are around 4-5% errors in correctly assigning the quality scores in the Indian fingerprints. It might be possible to tune the tool to Indian data.
- When the fingerprint images in DB1 (rural and urban setting), specifically those causing errors were analyzed, it was found that there are some specific causes that are more relevant in the Indian sub-continental region compared to Western and European countries. Lawsonia Inermis (commonly known as henna or mehandi) can cause significant differences in the quality of fingerprint images. Widely used by women in the Indian sub-continent during festivals, henna is applied on hand/fingers and when applied, fingerprint sensors may not properly capture fingerprint features.
- On analyzing the quality distribution of each finger in every age group, it is difficult to generalize little fingers as useful or not. Similarly, it is not possible to generalize that, a particular age group or gender conforms to lower or higher quality scores and hence better/worse performance.

Finally, it is strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out, to formally predict the accuracy of biometric systems for Indian rural and urban environments.

Face identification

Face image, uncorrelated to fingerprint image, can be utilized in two ways. Face image can be independently matched using automatic matching algorithm and the results fused together to achieve higher net accuracy. NIST reports improved accuracy using fingerprint and face image score fusion [28]. It should be noted that face image alone provides low accuracy rate. A more practical method is hierarchical matching where false match rate can be improved by comparing face images of suspected duplicates obtained in fingerprint matching. In the former, the entire database has to be used as gallery, making the matching prohibitively expensive. In the later, gallery size is small, typically 1% of database. The hierarchical method improves FRR (which reduces manual duplicate check) but does not directly improve FAR (which results in duplicates in the database). However, one can trade off FRR to improve FAR.

Iris

Iris has been shown to provide accuracy comparable to fingerprint. NIST Iris test provided accuracy rates shown in Figure 24[10]. T. Mansfield of National Physical Laboratory [33] reports low FAR for small sample.

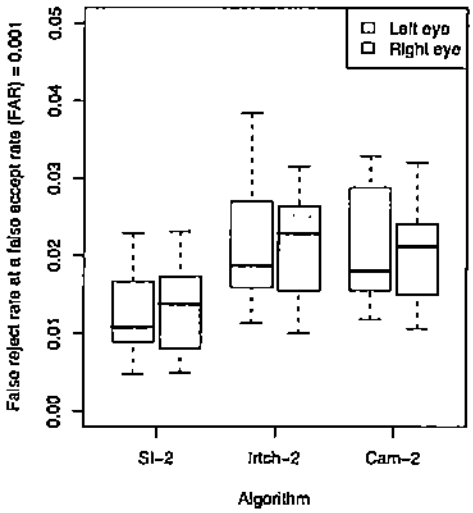


Figure 24 Iris FAR & FRR rate

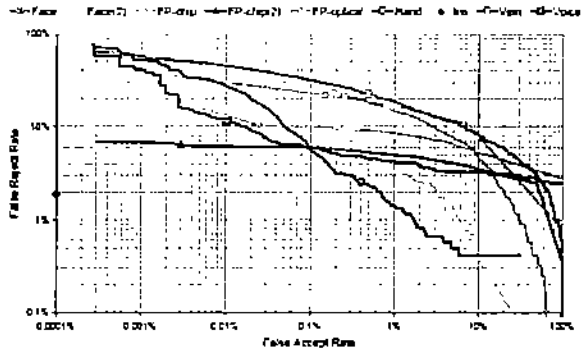


Figure 25 FAR and FRR of various biometric identifier

Fused Accuracy

A large body of literature documents the benefits of information fusion in a variety of fields including search, data mining, pattern recognition, and computer vision. Fusion in biometric is an instance of information fusion. A strong theoretical base as well as numerous empirical studies has been documented that support the advantages of fusion in biometric systems [1]. The main advantage of fusion in the context of biometrics is an improvement in the overall matching accuracy. Depending on the fusion method, the matching speed may also be improved significantly. Dr. Phalguni Gupta and his team report a study of fusion of fingerprint with iris [7]. They show a substantial improvement in matching accuracy by combining one iris with one finger. There is no empirical data available for Indian conditions though there is strong theoretical evidence that among all economically and technically feasible biometrics modalities,

combined fingerprint and iris has potential to provide maximum accuracy in Indian conditions.

ISO Documents

Included by reference

ISO/IEC 19794-2:2005. Biometric data interchange formats - Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats - Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

References

1. A. A. Ross, K. Nandakumar, A. K. Jain, Handbook of Multibiometrics, Springer, 2006
2. Anil Jain, Patrick Flynn, Arun Ross. Handbook of Biometrics, 2008
3. ANSI/NIST-ITL 1-2007. American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1
4. ANSI/NIST-ITL 2-2008. American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2 XML Version
5. Bolle, Connell et al. Guide to Biometrics, 2004
6. Fingerprint Image Data Standards for Indian e-Governance Applications, Draft Version 0.4, National Information Center
7. H. Mahrotra, A. Rattani, P. Gupta, "Fusion of Iris and Fingerprint Biometric for Recognition", Proceedings of International Conference on Signal and Image Processing (ICSIP 2006), Karnataka, India, 2006
8. IAFIS-IC-0100 (V7) Electronic Fingerprint Transmission Standard (EFTS) 1999
9. International Biometrics Group, "Independent Testing of Iris Recognition Technology, Final Report, May 2005", NBCHC030114/0002. Study commissioned by the US Department of Homeland Security.
10. IREX I, "Performance of Iris Recognition Algorithms on Standard Images", NIST Interagency Report 7629
11. ISO/IEC 19784-1:2006. Biometric Application Programming interface – Part1: BioAPI specification.
12. ISO/IEC 19794-1:2006. Biometric data interchange formats – Part 1: Framework
13. ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face image data
14. ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris image data
15. J. Cambier, "Iridian Large Database Performance", Iridian Technical Report 03-002
16. J. Daugman, "Algorithms, Performance & Challenges", BYSM, 2006
17. J. Daugman, "Iris recognition border crossing system in the UAE", International Airport Review (2) 2004.
18. J. Daugman, Technical Report 635, University of Cambridge, 2005
19. James Matey, "Iris Recognition", Sarnoff Corporation, BCC 2005
20. Jonathon Phillips, "ICE 2006 Large-Scale Results", NIST 7208, NIST, 2007
21. NISTIR 7110. Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints. C. L. Wilson, M. D. Garris, & C. I. Watson, May 2004
22. NISTIR 7112. Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB). Stephen S. Wood & Charles L. Wilson, April 2004
23. NISTIR 7123. Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, Charles Wilson etc al.
24. NISTIR 7151. August 2004 Fingerprint Image Quality
25. NISTIR 7201. Effect of Image Size and Compression on One-to-One Fingerprint Matching. C. I. Watson & C. L. Wilson. February 2005

26. NISTIR 7249. Two Finger Matching With Vendor SDK Matchers. C. Watson, C. Wilson, M. Indovina & B. Cochran. July 2005
27. NISTIR 7296. MINEX. Performance and Interoperability of the INCI TS 3 7 8 Fingerprint Template. Patrick Grother, Michael McCabe et al. March 2006
28. NISTIR 7346 TR. Studies of Biometric Fusion, 2007
29. Patrick Grother, Elham Tabassi, "Performance of Biometric Quality Measures", IEEE transactions on pattern analysis and machine intelligence, Vol. 29, No. 4, April 2007.
30. Registry of USG Recommended Biometric Standards, Version 2.0, NSTC
31. Report of the working group on standards for raw images of fingerprints, Reserve Bank of India
32. Shahram Orandi, Mobile ID Device Best Practice Recommendations, NIST Special Publication 500-280, August 2009
33. T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing Final Report", CESG Contract X92A/4009309, Centre for Mathematics & Scientific Computing, National Physical Laboratory, Queen's Road, Teddington, Middlesex TW11 0LW
34. UK Passport Service, Biometrics Enrolment Trial, May 2005

298

UIDAI

Unique Identification Authority of India
Planning Commission
Government of India

Approach Document for

Aadhaar Seeding

In

Service Delivery Databases

Version 1.0

Table of Content

1. Introduction

The Unique Identification Authority of India (UIDAI) has been created, with the mandate of providing a Unique Identity (Aadhaar) to all Indian residents. The UIDAI proposes to provide online authentication using demographic and biometric data.

Aadhaar seeding is a process by which UIDs of residents are included in the service delivery database of service providers for enabling Aadhaar based authentication during service delivery. As an example, MNREGA will require authentication before payout therefore in such a scenario, it will be essential to map UID of the resident with MNREGA Job Card number and other demographic information. Similarly, banks and insurance carriers may want to map Aadhaar numbers of all their customers. The objective is not to replace the currently used unique identifier of the customers/ residents/ beneficiaries with Aadhaar but the objective is to seamlessly enable Aadhaar authentication without impacting any other interface that the service providers maintain with their customers.

Aadhaar "authentication" means the process wherein Aadhaar Number, along with other attributes, including biometrics, are submitted to the Central Identities Data Repository (CIDR) for its verification on the basis of information or data or documents available with it. UIDAI will provide an online service to support this process. Aadhaar authentication service only responds with a "yes/no" and no personal identity information is returned as part of the response.

2. Terminologies

Before reading the document, it is important that the terms mentioned in this section are understood very well as they are used very frequently in subsequent sections without any further explanation.

Terminology	Description
EID UID Mapping XML file	A file generated by the CIDR after creation of Aadhaar number. It contains one or more pairs of EID and UID related to residents enrolled by a registrar. This file is available on Aadhaar portal for download by registrars and their authorized representatives
KYR	KYR is a set of mandatory information pertaining to residents. It includes mandatory details like Name, Date of Birth/ Age, Address and Gender along with few optional fields like email Id, mobile number etc.
KYR+	This is the additional information, apart from mandatory KYR, captured by the registrar at the time of enrolment. Ex. MGNREGA Job Card Number, Ration card number etc.
Service Delivery Database	Database containing resident records among other types of master data/ transactional data which a service provider maintains to deliver its services. Ex, Ministry of Rural Development maintains a database which contains resident records in rural areas to operationalize the MGNREGA program

3. Aadhaar Seeding Strategy

At the outset, it is to be noted that strategy for Aadhaar seeding is a combination of several sub-strategies and no one solution will apply to all cases. Therefore it is essential that every seeding process is thoroughly analyzed and planned before proceeding with actual seeding. While it is the responsibility of the service providers to seed their service delivery databases with Aadhaar, UIDAI will support by providing necessary tools, expertise, best practices and consulting advisory on request.

Why Aadhaar Seeding is required

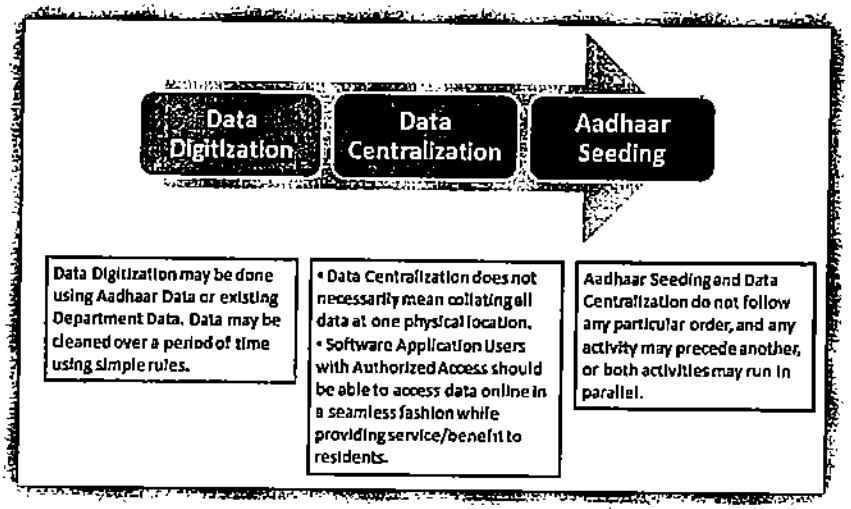
Going forward, Aadhaar will form the basic, universal identity infrastructure over which registrars, government and other service providers across the country will be able to build their identity-based applications. These features in turn are expected to serve a developmental mandate to potentially achieve multiple transformational benefits of development and equitable growth through:

1. Proper identification leading to better targeting of development schemes provided by government and private sector
2. Ensuring that all fake, duplicate and ghost records are weeded out from databases so that leakages resulting from such records are avoided.
3. Increased reach and efficiency in delivering many goods and services like PDS, banking and financial services, telecom, health, insurance, education etc.
4. No repeated KYC checks for residents

One critical input for leveraging Aadhaar authentication is Aadhaar number (UID) itself which needs to be captured and stored along with the current unique identifier (*Customer Id/ Beneficiary Id etc.*) in service delivery databases. At the time of authentication, the mapped UID in service delivery database will be used to authenticate therefore it is essential that Aadhaar seeding is performed.

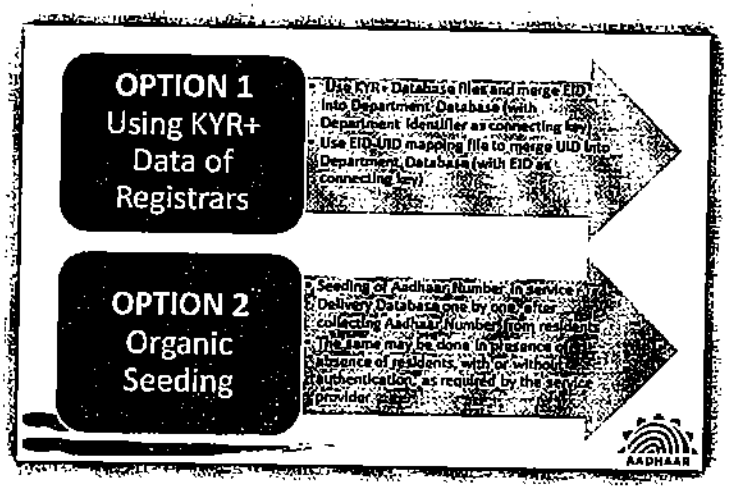
Pre-requisites to Aadhaar Seeding

Refer the diagram here; seeding process has to be necessarily preceded by Data Digitization and Data Centralization.



Data Digitization essentially means collation of service delivery data in an electronic format (database/excel or similar) from where data can be retrieved using standard

SQL queries. UIDAI suggests use of a RDBMS (MySQL/ SQL Server/ Oracle/ Sybase/ DB2 and similar). It is also important that personal identity data slowly becomes consistent across multiple systems. Aadhaar is also an initiative to standardize personal identity information, and Aadhaar data may be used to clean the existing data.



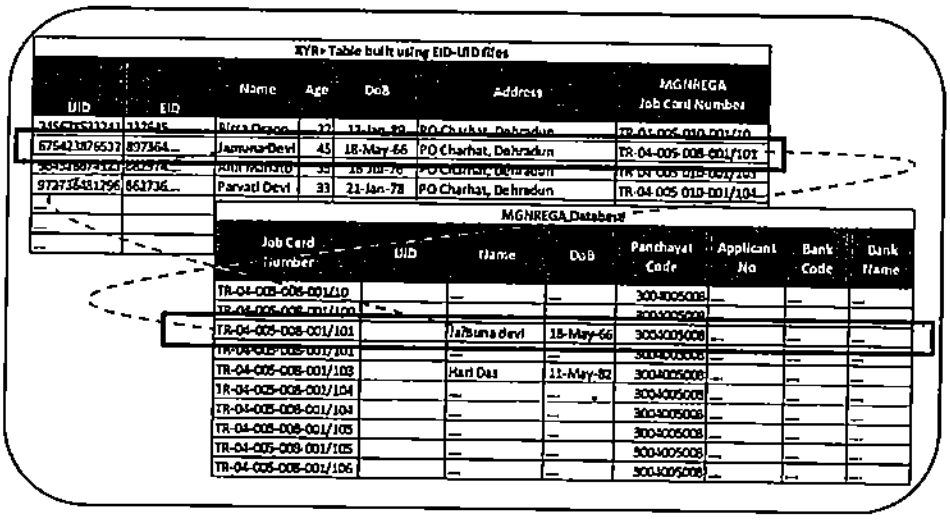
Data Centralization primarily manages availability and accessibility of distributed service delivery data. The objective here is that the seeding process/ utility should be able to access the service delivery data and all related information in at least the read-only mode. Example: In a state, pensioners' data may be available in data silos across districts. A consolidated view of the entire data would facilitate the social welfare department of the state to improve the service delivery in their programs, while also being able to ensure that the same person is not availing double benefits from two different districts. In case, service delivery data is already digitized and centralized then no action is required from seeding perspective.

Seeding Strategies

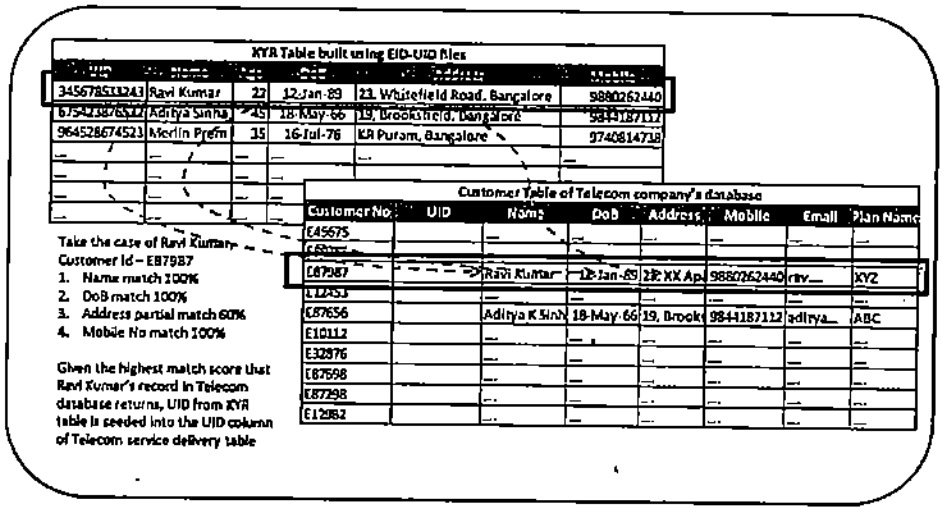
Primarily there are two ways of seeding of service delivery database with Aadhaar number, *Top-Down method* and *Organic method* where former method uses enrolment information, available in KYR+ and EID/UID files as input whereas latter requires the service provider contact the resident or vice-versa for updation of Aadhaar number, after the resident goes through a seeding process decided by a service provider.

Top-down Seeding

This is a method by which one or more KYR and KYR+ fields in KYR+ database are compared with the equivalent fields in service delivery database in order to find a suitable match. Upon finding a match Aadhaar number from KYR+ database is seeded into the service delivery database. Consider an example where MGNREGA Job Card number was captured as KYR+ field at the time of the enrolment. The field Job Card Number along with resident name can then be used to find a matching unique record in MGNREGA database. Below diagram illustrates this scenario:



Another possible scenario is where there is no relevant KYR+ field captured, example customer Id with a telecom company. In such cases, one or more KYR fields should be used for matching



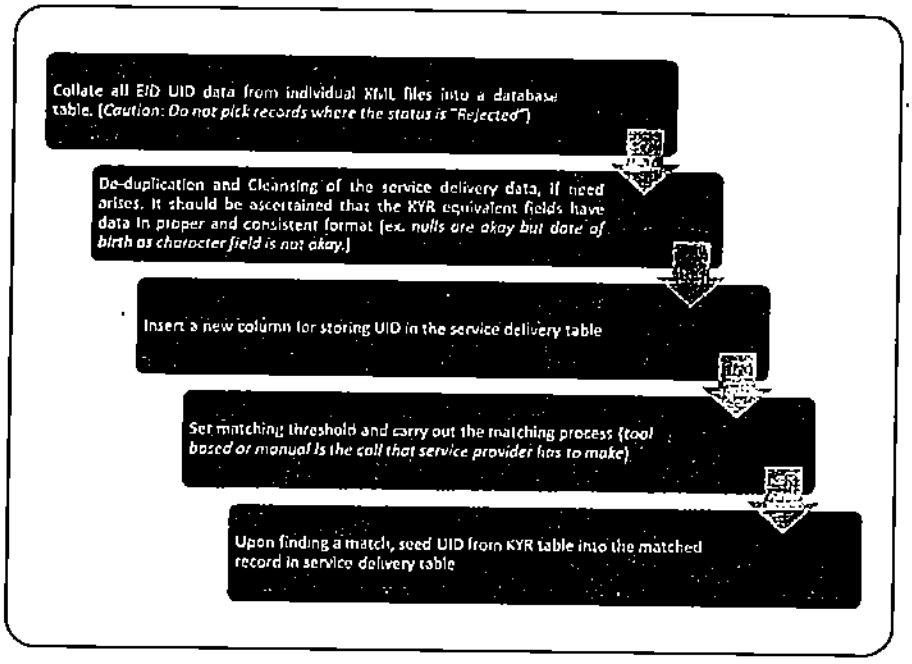
As shown above, KYR fields (Name, DoB, Age, Address) from KYR Table are matched with the KYR equivalent field in the service delivery table and based on the match percentage of individual fields, an overall match score is calculated. It is ideal to have 100% match for seeding to take place but that happens rarely therefore it can be assumed that if the match score exceeds a pre-defined threshold (possibly 80%) then a match may take place.

In the diagram above KYR table, built using EID-UID XML files, has been used as reference table, however reference database can also be created using KYR+ data as well. Advantage of using KYR+ data is that it always contains KYR data, except the UID, along with additional information as mandated by the registrar. As an example, registrars may make it mandatory to capture residents' MGNREGA Job Card number or PDS Ration Card number at the time of enrolment. Capturing of additional information

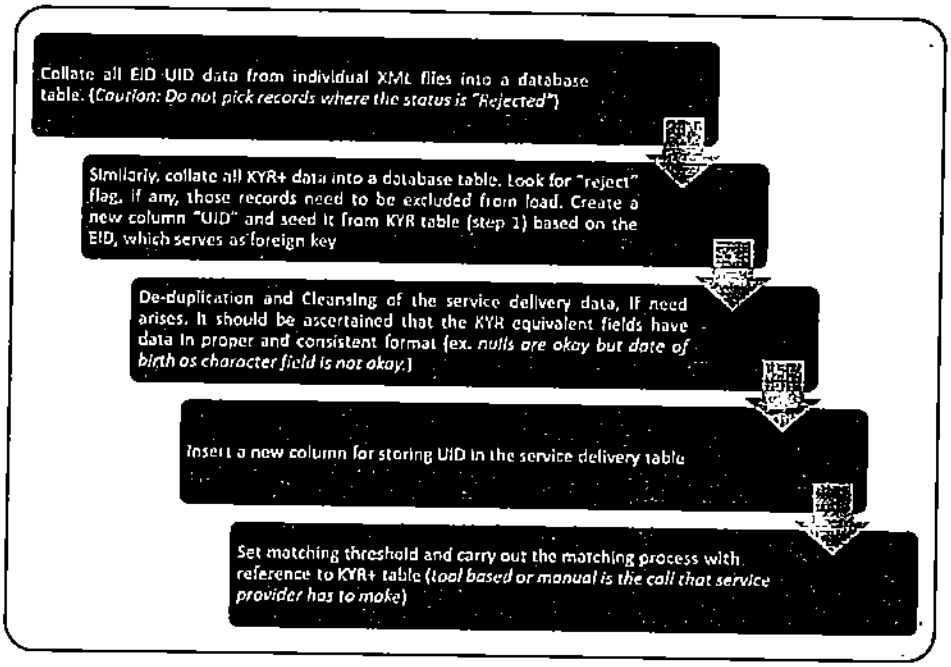
makes seeding simple as unique identifiers thus captured can be used for matching of records between KYR+ and service delivery tables whose unique has been captured as an additional information during enrolment – a Job Card number or Ration card number or any other unique identifiers are ideal conditions for matching to take place.

Execution Steps

Execution steps indicated below assume usage of *Ginger*, seeding utility developed by UIDAI in-house. Refer Appendix-1 for details related to the tool. Below diagrams gives step-wise approach of seeding using KYR and KYR+ data



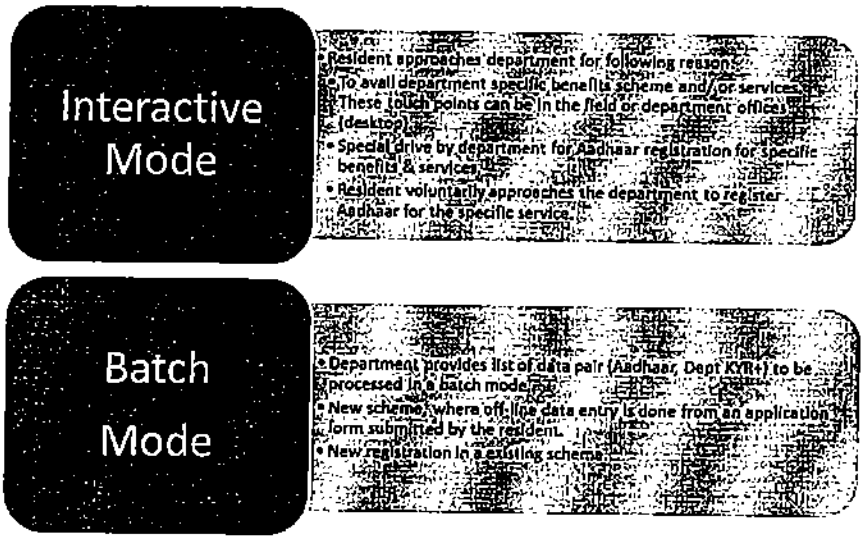
Seeding using KYR Data (obtained from EID-UID XML files)



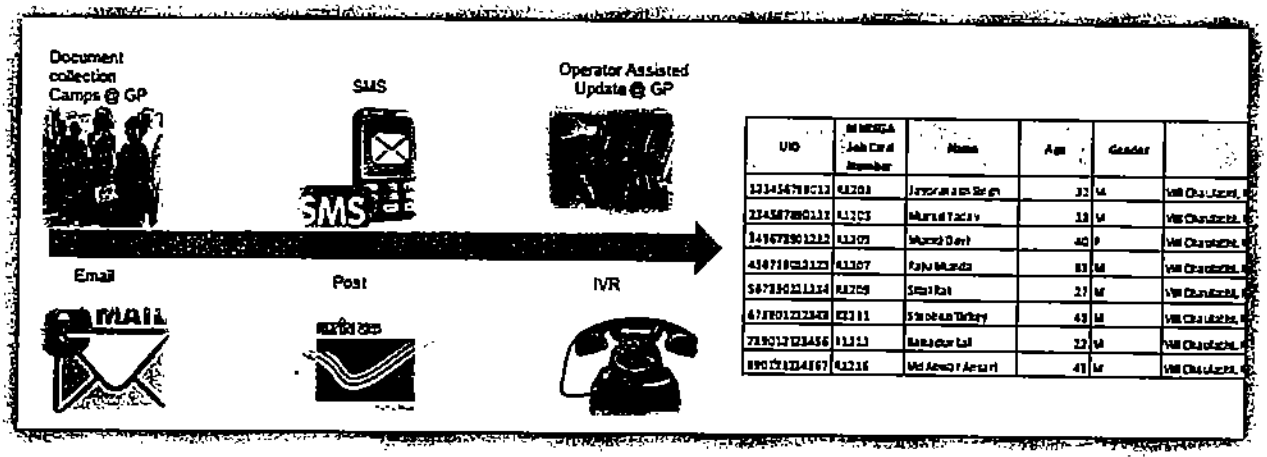
Seeding using KYR+ Data

Organic Seeding

Organic seeding is a method which involves creation of touch points with the residents where the residents voluntarily or in response to service provider's call initiate inclusion of their UID in service delivery databases. This approach can be implemented in an interactive mode or in batch modes.



The touch points, as mentioned above can be created in various ways as illustrated below. A department can leverage one or more channels of communication with the residents in order to capture their Aadhaar numbers



UID	MGNREGA Job Card Number	Name	Age	Gender	
123456789012	RJ2701	Jamnalal Ram Singh	32	M	Vill Chandpura, P
234567890123	RJ1705	Munni Devi	28	M	Vill Chandpura, P
345678901234	RJ1709	Mukesh Dixit	40	M	Vill Chandpura, P
456789012345	RJ1707	Raju Mundra	33	M	Vill Chandpura, P
567890123456	RJ1705	Shiv Rai	27	M	Vill Chandpura, P
678901234567	RJ1711	Shankar Dhakay	43	M	Vill Chandpura, P
789012345678	RJ1713	Babulal Gal	22	M	Vill Chandpura, P
890123456789	RJ1716	Md Akram Ansari	41	M	Vill Chandpura, P

Channel	Description
Document Collection at touch points	Residents are expected to hand over copies of Aadhaar letter and registration form with the service provider (ex. Ration card). Service provider later updates the service delivery database based on the information supplied
SMS	Service provider enables a SMS based application. Residents are expected to send a SMS containing the Aadhaar number and registration number with the service provider. Ex *UPD <Aadhaar Number> <Ration Card Number>* is sent to a number *59999* (illustrative only). The application at the backend seeds the Aadhaar number into the database by using the Ration Card number as key. For verification of information supplied service provider needs to conduct demographic authentication post seeding (discussed later)
Operator assisted update @ touch points	Service provider enables direct seeding of Aadhaar number at resident touch points where residents are expected to come along with supporting documents – Aadhaar letter and service registration document. The resident is authenticated both demographically and biometrically before Aadhaar number of the resident is seeded in service delivery database
Email	Similar to the SMS based approach. Email needs to be sent to an email id in a pre-defined format along with scanned copies of supporting documents as attachments. Upon receiving the email, the backend application extracts required information from the email and seeds database appropriately. In case of a failure, resident is informed by a reply email
Post/Courier	Similar to Document collection approach, however in this case collection of documents happens through post/ courier
IVR	A telephone based IVR application that captures Aadhaar number and Registration number in an interactive manner. Upon capturing the required

Channel	Description
[redacted]	information backend application seeds service delivery database appropriately. Demographic authentication should be conducted post seeding for verification
Self-service Web Portal	Service Provider may open up a web portal for residents to update their Beneficiary Identifier Number / Account Number, along with Aadhaar number. Service Providers may do a demographic authentication at the back-end before updating their database with Aadhaar number.

Refer Appendix 2 for a detailed approach of seeding Aadhaar into bank's database by means of ATMs and micro-ATMS.

Demographic and Biometric Authentication

After the completion of Top-down seeding and Organic seeding where no direct update of service delivery database was enabled, it is highly recommended that demographic authentication of data in service delivery database is conducted. This is to ensure that seeding has indeed been done correctly. In cases where demographic authentication fails, service provider should investigate into the reasons of failure of authentication. Some of the reasons of failure are:

1. Aadhaar seeded into an incorrect record. This may potentially happen in the cases of partial or fuzzy match
2. Resident updated his/ her KYR data in CIDR (due to marriage, change of address, updation of incorrect information)
3. Incomplete or incorrect KYR+ data captured during enrolment (ex. incorrect MGNREGA Job card number)

Enabling of Biometric authentication is required at operator assisted touch-points where a direct update of service delivery database takes place.

Refer Ginger, seeding utility, in Appendix-1 for more details on usage of demographic authentication module.

A pre-requisite to conducting Aadhaar authentication is that the service provider should be an AUA (Aadhaar User Agency).

Authentication User Agency (AUA): An organization or an entity using Aadhaar authentication as part of its applications to provide services to residents. Examples include Government Departments, Banks, and other public or private organizations. All AUAs (Authentication User Agencies) must be registered within Aadhaar authentication server to perform secure authentication.

Sub-AUA (SA): An organization or a department or an entity having a business relationship with AUA offering specific services in a particular domain. All authentication requests emerging from an AUA contains the information on the specific SA. For example, q specific bank providing Aadhaar enabled

payment transaction through NPCI as the AUA becomes the SA. Similarly, a state government being an AUA can have the health department under them as the SA using Aadhaar authentication while providing healthcare benefits.

Authentication Service Agency (ASA): An organization or an entity providing secure leased line connectivity to UIDAI's data centers for transmitting authentication requests from various AUAs. All connections to production authentication servers must come through private and secure connection through ASAs. Those AUAs who wish to provide their connectivity can become their own ASA whereas smaller AUAs who do not wish to create direct leased line connection to UIDAI's data centers can use an ASA.

Common Challenges during Seeding

It is important to understand the common challenges during seeding so that necessary precautions can be taken early during planning. Below are the some of the challenges that seeding team should be aware of and develop necessary processes/ workarounds to overcome them.

1. **Complete data is not captured in service delivery databases:** Data is often entered manually by semi-skilled data entry operators which results in incomplete and incorrect data. Lack of adequate QA process by service provider too contributes to the problem. Data digitization strategy should address this potential issue
2. **Similar information across different data sources do not have exact match between them:** It has been observed that same data across different tables are not entered similarly. Take the case of names *MV Ramachandran* and *Madanapalli Venkata Ramachandran* that refer to same person. Seeding involves exact/ partial match of various data fields therefore such issues should be handled during data cleansing and normalization
3. **Data in service delivery database is in a local language:** Matching of data in same language can be done with standard comparison algorithms but if the language (e.g. भारत vs. India) no way a match can be made. If a match is to be made then the algorithms need to be made extremely intelligent and complex unless data level changes made in the database
4. **All the required data is not available:** Careful planning and coordination with support groups need to be done. As an example, codec information should be made available in cases where only codes are stored (often in Gender field, Male is stored as 1 and Female as 2)
5. **Normally available tools become incapable to handle high volume of data:** Normally everyone prefers using Microsoft Excel for data handling. However, it has been observed that after few thousand records inserted into excel sheet, response time of the tool deteriorates significantly. In such cases alternatives like use of database tools should be thought of – e.g. import data into a database (MySQL, MS SQL Server, Oracle so on and so forth)
6. **Mobilization of Residents:** In the case of *Organic Seeding*, mobilization of residents is required in order to complete seeding. Multi-channel organic seeding approach needs to be employed for effective mobilization

As stated earlier, it is recommended that seeding teams share their experience with UIDAI team (*rakesh.ranjan@uidai.gov.in*) at HQ, Delhi so that seeding approach/ methodology, learning and best practices can be published to other teams involved in seeding.

4. Case Study 1 – Seeding of Aadhaar in RoR @ Tripura

Owner Organization	Govt. of Tripura
Scope of Work	Seeding of Aadhaar number into RoR (Register of Ordinary Residents) database
Location	Agartala
Schedule	Nov '11 to Mar '12
Stakeholders	1. Government of Tripura 2. UID Authority of India 3. NIC
Roles and Responsibilities	Gov. of Tripura (GoT), owner of the project 1. **NIC** -Provide access to RoR database 2. **Registrar** - Provide EID-UID files and KYR+ files available with the registrar 3. **GoT** - Provide necessary hardware and software licenses to execute the seeding process 4. **GoT** - Provide leadership support in resolving bottlenecks 5. **GoT** - Provide data entry operators for data entry into RoR 6. **GoT** - Execute seeding steps 7. **GoT** - Prepare Data Digitization Strategy 8. **GoT/ NIC** - Prepare Data Centralization Strategy 9. **GoT/ UIDAI** - Prepare Seeding Strategy UIDAI, the implementation partner 1. Participate in analysis of enrolment and RoR data 2. Conduct trainings for the seeding execution team 3. Provide oversight during seeding 4. Conduct post-seeding review 5. Prepare closure report
Digitization Strategy	Tripura is one of the few states that have taken the initiative to create a register of all residents in the state called RoR (*Register of Ordinary Residents*). As part of this program it is intended that details of all 35L residents of the state are stored in one database. Therefore from digitization perspective, the state is doing everything right except for the fact that only 9L/35L records have been created in RoR as of Oct '11.

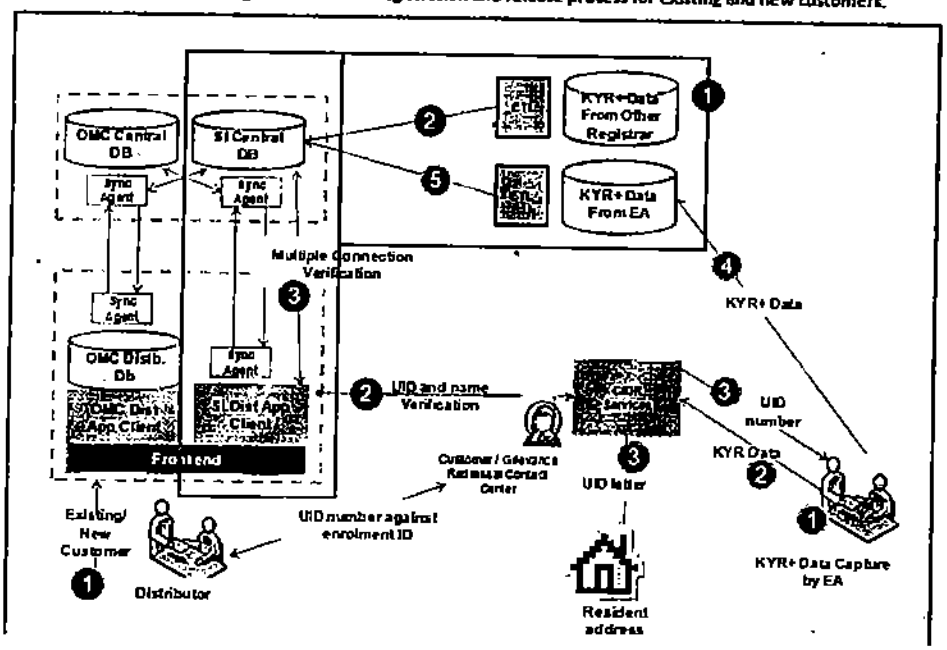
	It is expected that by April 2012 records of 35L residents will be digitized
Centralization Strategy	In order to carry out seeding process, KYR, KYR+ and RoR data will be needed. EID-UID files will be used to obtain KYR data while KYR+ .mdb database files will be used to obtain KYR+ data. Access to RoR database and data dumps has already been provided by the Gov. of Tripura. Using the EID-UID extractor program, KYR data that includes UID as well will be extracted and uploaded to a SQL Server database. All KYR+ .mdb files be merged to create one database on the same SQL Server instance
Seeding Strategy	It has been proposed by GoT that seeding should commence from Gram Panchayats so that the welfare programs targeting rural population, ex MGNREGA, are benefited before any other program. Below flow diagram explains the complete seeding strategy **RoR Data Cleansing** • Ensure all the names are entered in Bangla. There were few cases where names were entered in English • Ensure all the DoBs are entered as a date. In case only the age is known then convert that to a date as "1/1/<derived year>". Ex 34 years of age will be converted to 1/1/1977 • De-duplication of records, Panchayat-wise **Seeding** • For every record in KYR+ database, based on the EID find the UID in EID-UID database. Update the record • Split by means of database query the RoR records Gram Panchayat-wise • Using Ginger, for every record in step 2, match the resident name and location id in the KYR+ database • Manually select the matching records by verifying the name, date of birth, address and other possible fields • Mark the record as seeded **Demographic Authentication** • Post seeding , run the demographic authentication utility available in Ginger to validate seeded data • In case of demographic authentication failure mark the records for review • Re-run biometric authentication post review of such records
Tools	Ginger with MSSQL Server database, RoR on MSSQL Server database, Excel
Risks/Mitigation	1. As of Oct 11 coverage of RoR is approx. 50% of state's population. All the analysis and recommendation is based on this set of data. New issues not observed so far that might come later will potentially impact the seeding strategy
Issues/ Resolution	**Issue**: In significant number of RoR records date of birth recorded as year only **Resolution**: 1. Converted data type of field to 'Date'. 2. Converted all variants of DoB to

		dates. Ex 1956 was changed to 1/1/1956 3. Different date formats were changed to one format of "yyyy-MM-dd" for consistency and enabling matching using this field
	Only first 14 digits of EID captured in RoR	No change to EID field but this EID with Name, DoB gave a unique match
Best Practices	1. Involvement of Panchayat level officials for seeding and verification post-seeding. This approach is based on the assumption that Panchayat leadership is aware of every resident in its area of operation 2. Start small and then expand. Began seeding of data pertaining to Panchayats with population not exceeding 1500. This helped in identifying the ground level challenges and thus identifying mitigation strategies	
Learning		
Assets shared/ can be shared with UIDAI		
IPR Details		
Point of Contact	Mr. Kiran Gitte, IAS DM and Collector West Tripura District Agartala Mr. Rakesh Ranjan Senior Manager (Applications) UID Authority of India	

5. Case Study 2 –Aadhaar enabled LPG Delivery pilot with IOCL

Scope of Work	1. Integrate Aadhaar in Oil Marketing Companies Database to remove, duplicates and ghost 2. Perform Aadhaar based Biometric Authentication at time of delivery of cylinder
Location	Mysore, Hyderabad and Pune
Schedule	As of Feb 2012 - In Progress
Stakeholders	• UIDAI • Residents (Consumers of LPG) • OMCs • OMCs' Distributors
Roles and Responsibilities	• UIDAI - to provide Authentication Service • OMC - to build a system for Aadhaar Integration across OMCs • Distributor - to perform authentication at time of delivery with Pos Device • Resident (LPG Consumer) - to provide Aadhaar number and to participate in biometric authentication at time of acceptance of delivery.
Digitization Strategy	Oil Marketing Companies have over many years undertaken various computerization initiatives for delivery of Domestic LPG. Indian Oil Corporation Limited uses software package called 'Indsoft', Bharat Petroleum Corporation Limited uses 'nLPGnext' and Hindustan Petroleum Corporation Limited uses 'DCMS'. Through these initiatives, digitized customer data was already available with OMCs. OMCs had to seed in or rather associate Aadhaar data with its customer database. OMCs developed a common integrated database which associated Aadhaar numbers of connection owner, family members and authorized representative with identified unique key for each customer of OMC for domestic LPG. Identified Unique key (Candidate Primary Key) was used for all business transactions and Aadhaar was used for biometric authentication
Centralization Strategy	All OMCs customer databases to talk to each other, for removing duplicate across the OMCs. SI hired to build the integration software

Envisaged scenario for UID aligned connection registration and release process for existing and new customers.



Seeding Strategy

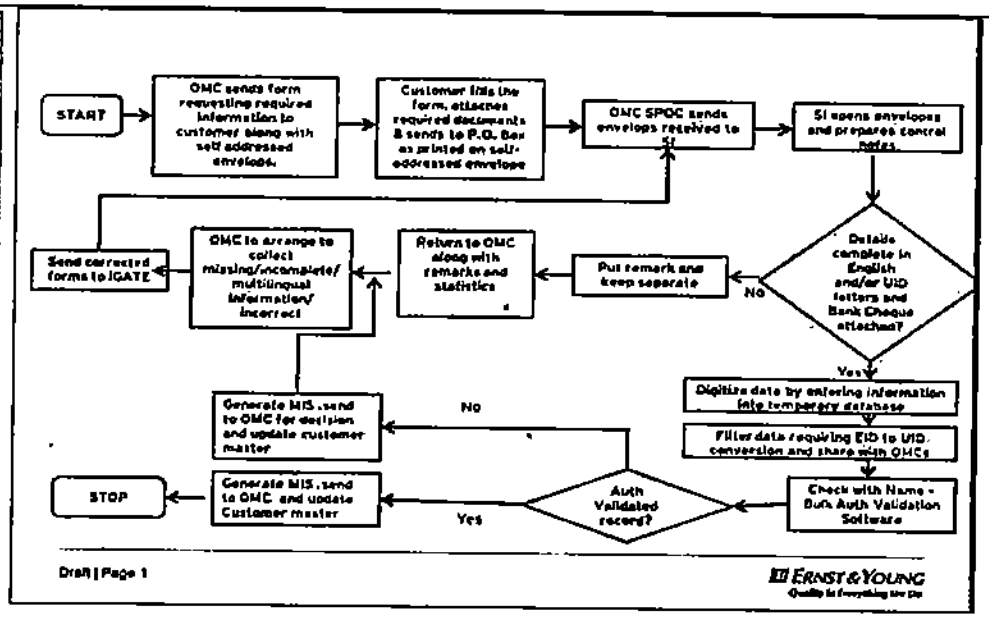
OMCs originally planned for three pronged strategy:

- Associating Aadhaar data from KYR+ data received from Enrolment Agenc(ies);
- Associating Aadhaar data from KYR+ data received from other Registrars;
- Organic seeding of the data

For Pilot, only Organic seeding was undertaken because

- OMCs did not appoint Enrolment Agencies in cities identified for Pilot as other Registrars were already present for enrolments
- KYR+ data received from other Registrars had very small subset of LPG customers providing information sought by OMCs

Following is the process being followed by OMCs for organic data seeding



Tools

1. Separate database associating Connection Owner details and Aadhaar numbers
2. Manual Excel based entry for Aadhaar numbers for self, family and authorized representative
3. Batch upload utility for uploading the Aadhaar data
4. Bulk Demographic Authentication with CIDR of Aadhaar data collected
5. EID to UID update through excel macros
6. Batch upload of validated data

Risks/ Mitigation

SL No	Risk	Mitigation Strategy
1	Delay in mobilization of customers to provide UID details	Proper communication plan for the customers
2	Incomplete forms submitted by customers	Re – approaching the customers to submit the data
3	Misplacing of envelops	Tracking of envelops
4	Form filled in local language	UID letters asked to be attached along with the form .
5	Incorrect UIDs entered in the Form	Shall be filtered out during demographic bulk authentication

	6.	EID provided	EID to UID conversion through macros
	7	Incorrect UID data entry	Shall be filtered out during demographic bulk authentication. Need to be verified with hard copies. If found incorrect in hard copy as well, need to approach the customer for providing the data again.
	8	Bulk demographic authentication failure	Need to be verified with hard copies. If found incorrect in hard copy as well, need to approach the customer for providing the data again.
	9.	Non availability of KYR+	Fall back on Organic seeding
	10	Incomplete availability of KYR+	Fall back on Organic seeding
	11	Low percentage of enrollers providing KYR+	Fall back on Organic seeding
	12	Customers not attaching UID letters along with the forms	Depend on hard copies for information. If found incorrect in hard copy as well, need to approach the customer for providing the data again
	13	Customers non willingness to provide information/fill the form	Plan for various modes of providing UID information e.g. website, sms etc.
Issues/ Resolution			
Best Practices	**Start small and expand** The project involves three OMCs viz. IOCL, BPCL and HPCL, Different Databases/ Database schemas amongst the three OMCs, Different System architecture for each OMC, Different software application implemented at each OMC, Receipt of KYR+		

	input data from Enrolment agencies and other Registrars To achieve an effective data migration procedure, data in the existing IT systems needed to be associated and uniquely identified through system developed by the SI (System Integrator). Accordingly data was mapped to the new system providing a design for data extraction and data loading. **Data Migration strategy** Following is the three-pronged strategy which was adopted for the data migration for OMCs: a) **Incremental cutover:** Since the current project is a pilot for a subsequent nationwide rollout, the data will be moved to the target environment by migrating only discrete parts of the business and associated data. However, current data in existing systems will continue to co-exist. b) **Data Enrichment (KYR+ association):** Manual intervention was required for this step followed by a maker checker control to check the integrity of the enriched data. Also, temporary storage solution was used that allows users to extract data from legacy system (s) and perform various transformations to get it into a fit state for loading into the target environment. c) **Bi-directional Synchronization:** Changes in the old system were allowed to flow to the new target system and changes to the target system to flow back to the old system. Since, there is an envisaged update to customer record, that is, addition of customer UID, household or family details & their UIDs, nomination of authorized personnel & their UIDs; it was needed to post connection owner's UID changes back to the old system that performs legacy operations on same account.
Learning	**Start early** As done in OMCs, data digitization process should be started early in the project so that by the time application development is complete and stabilizes, sufficient data is available in the system for testing. **Streamlined Digitization process** Streamlined flow for data digitization should be in place when multiple stakeholders are involved, with clearly defined roles and responsibilities. **Periodic MIS** Periodic MIS to track flow of data digitization and snapshot into data digitization process helps monitoring digitization activities. MIS was sought containing following information a) Tracking of communication sent to customer b) Tracking of envelops received c) Tracking of digitized data d) Tracking of non-digitized data along with reasoning
Assets shared/	1. Customer Form

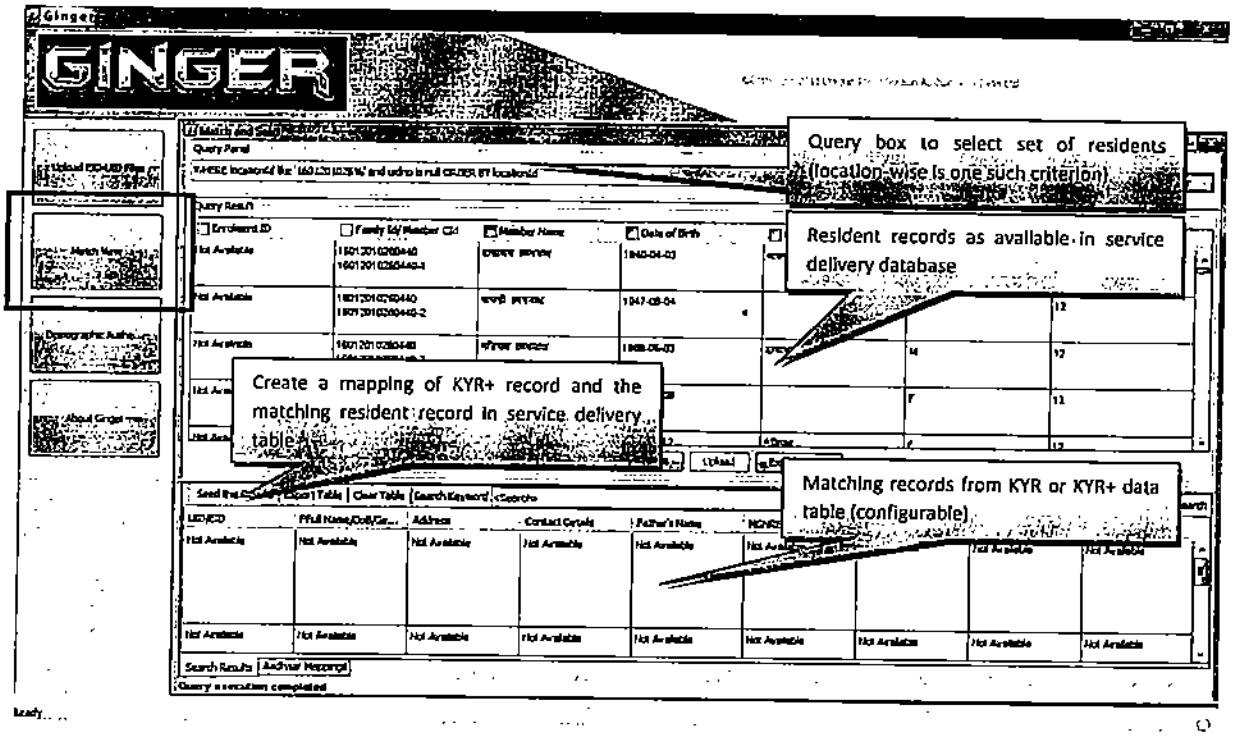
can be shared with UIDAI	2. System Requirement Specification 3. Functional Requirement Specification 4. MIS Template 5. Digitization Templates/ Formats
IPR Details	
Point of Contact	Mr. P Jayadevan Chief Manager, LPG sales, IOCL ** email Id will be provided on request*

6. Appendix 1 - Ginger (Seeding Utility)

Seeding process typically involves data extraction, consolidation, normalization and matching. For performing these activities, UIDAI has developed **Ginger**, an in-house tool which can be used by service providers after signing an agreement with UIDAI in order to ensure that the tool is not used for purposes other than intended for. Features of this tool include

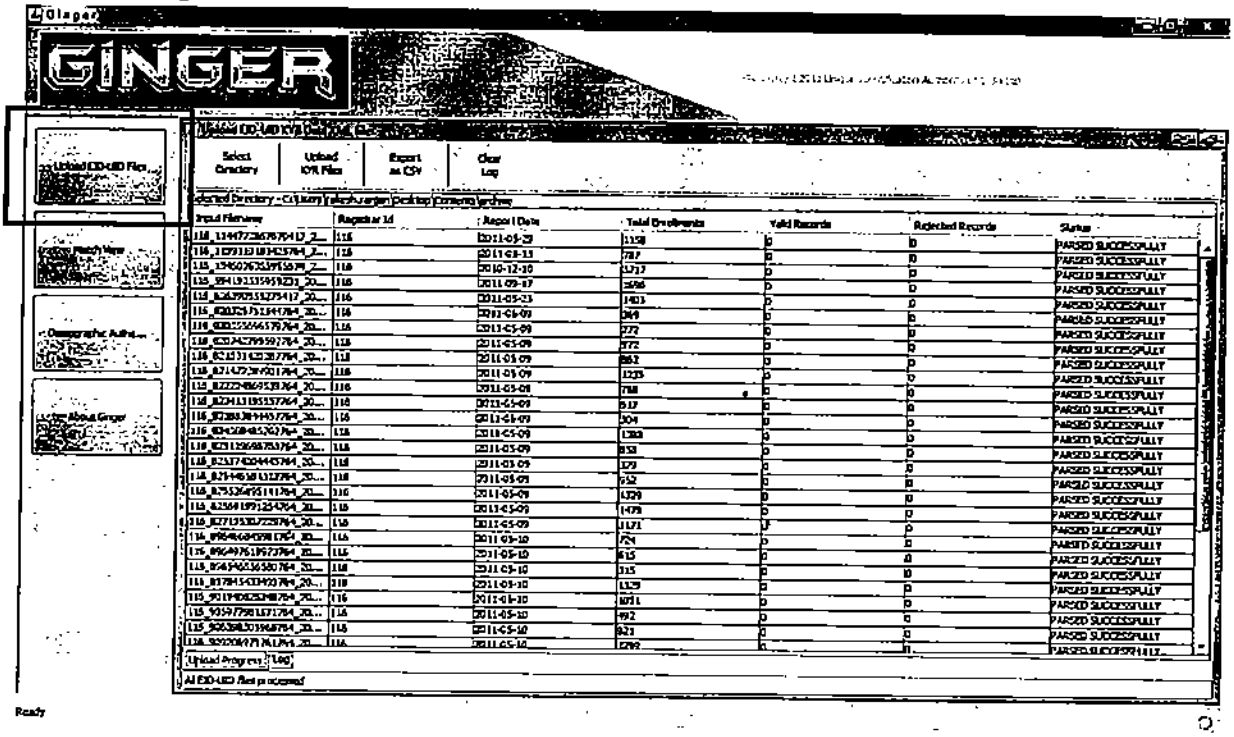
Feature	Description
Extract EID-UID Data	Extracts node data from EID-UID XML files and inserts into a database. It helps build the reference tables that contains all the UID generated along with KYR data for the target population
KYR+ merge utility	KYR+ files are generated in various formats e.g. txt, mdb etc. In the current release the tool will be able to handle only the mdb files however support for other formats will be added later
Matching Utility	This utility can help in identifying matching records across service delivery database and KYR+ database. Upon finding match, user can mark the matched record which can be then used to generate a SQL script for actual database update post QA review of mappings by a competent authority. *Important: This tool does not perform automatic seeding owing to security reasons*
Demographic Authentication	This utility is not available in the current release. Objective of the tool is to perform authentication on demographic data after completion of seeding. Successful authentication would mean that the resident/ customer data in service database has been synced up with data in CIDR

Match and Seed Module



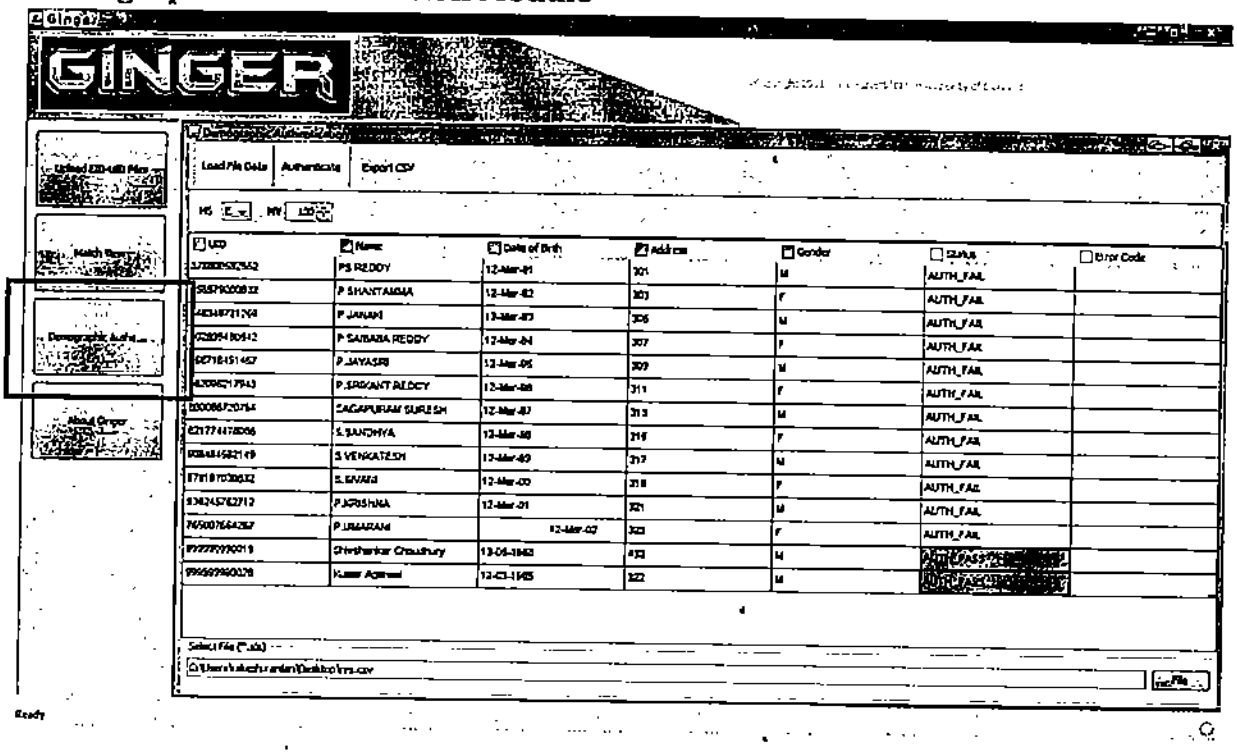
Using this module, one or more KYR equivalent fields (Name, Date of Birth, Age, Gender) from resident records in service delivery database are matched with equivalent fields in KYR+ or KYR records (configurable) - refer the user manual for usage guidelines. The mappings thus created can be exported to excel for further review and approval by a competent authority appointed by the service provider. It is to be noted that functionality of match and seed module is limited only to creation of mappings and their export. It is expected that based on mapped data, service providers create custom SQL scripts to update the service delivery database

EID-UID Upload Module



With the help of this module, EID-UID data from XML files can be uploaded into any database (currently mapped to MySQL). It is a multi-threaded utility that simultaneously uploads data from all files resulting in very fast upload (*on a normal workstation it takes less than 3 min to upload 30,000 records*). It also produces a reported that contains information related to number of files successfully read, total records read, total number of records inserted and total number of records rejected.

Demographic Authentication Module



In order to verify whether seeding has been done accurately, it is essential that the resident records in service delivery database are authenticated demographically. Objective of demographic authentication is to check whether UID and KYR fields are mapped correctly and are in line with the data in CIDR.

Post demographic authentication, "Status" column is updated with one of the authentication statuses "AUTH_PASS"/"AUTH_FAIL"/"AUTH_ERR". In the case of AUTH_FAIL or AUTH_ERR, error code is also indicated that explains the reason for authentication failure which can be used for investigation purposes.

Pre-requisites for conducting demographic authentication are:

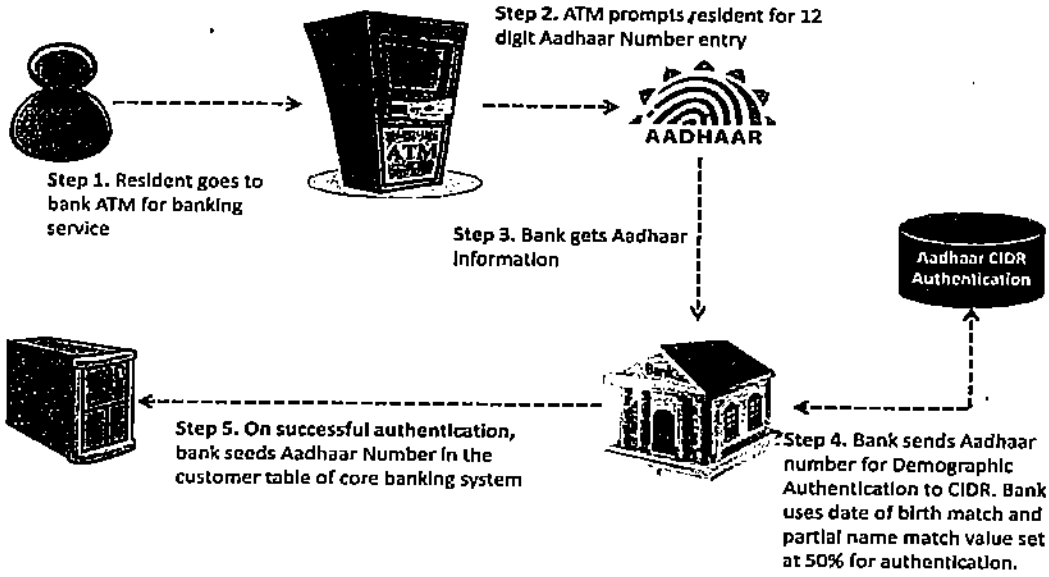
1. Service provider/ government agency has assumed the role of AUA
2. The agency has either assumed the role of ASA or entered into an agreement with another ASA for routing of authentication requests to CIDR
3. AUA application has been developed that complies with the specification outlined in the authentication API document (*http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_5_rev1_1.pdf*).

The above pre-requisites are mandatory because access to CIDR production data will not be available to requesting agency otherwise.

7. Appendix 2 – A Bank's approach to Organic Seeding

Banks may use ATM's and going forward, Micro ATM's to seed Aadhaar numbers of their customers. ATM's and Micro-ATM's are the best touch points for bank customers. The following diagram shows the seeding of Aadhaar numbers by a bank through its network of ATMs.

Steps for ATM based seeding



Steps for Micro-ATM based seeding

1. Resident should be able to provide three things which may be captured on the micro-ATM device namely Aadhaar number, Bank Account Number and Bank's BIN number. The device may maintain the mapping of bank name and BIN number, since resident may not know BIN number. (Name capture may be optional)
2. Creation of CSV files at the end of the day (or at any other time period) with list of all records captured so far, which can be exported from the device onto a laptop/computer. The file-name should reflect the export date-time
3. Ability to push the relevant records/CSV to corresponding bank based on BIN number. The banks should open interfaces to accept such records in a CSV
4. Banks may do a demographic authentication with partial match (let's say 50 percent) before seeding the Aadhaar number in core banking system database
5. If banks maintain mobile numbers of customers, they should send an SMS to its customers with the update. "*Your Aadhaar number XXXX XXXX 5302 has been linked to your bank account number XXXX XXXX 1185. Please contact us in case of any queries*".

322

सत्यमेव जयते

Aadhaar

Authentication Implementation Model

Operating Model

Version 1.0

AADHAAR

Unique Identification Authority of India
(UIDAI)

Table of Contents

Abbreviations and Terms

UIDAI	Unique Identification Authority of India
CIDR	Central Identities Data Repository is a logical collection of one or many UIDAI data centers where the central technology infrastructure required to issue Aadhaar numbers, update resident information, and authenticate the identity of residents is available.
FalseReject	The instance of a system failing to detect a match between the input pattern and a matching template in the database
FRR	False Reject Rate – the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
False Accept	The instance of a system incorrectly matching the input pattern to a non-matching template in the database
FAR	False Accept Rate – the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.
PID	Personal Identity Data
PII	Personal Identity Information (or Personally Identifiable Information)
ICDS	Integrated Child Development Services
JSY	Janani Suraksha Yojana
KYC	Know Your Customer
KYR	Know Your Resident
MSP	Managed Services Provider is an entity proposed to be appointed for management of CIDR
NREGA	National Rural Employment Guarantee Act
PDS	Public Distribution System
RSBY	Rashtriya Swasthya Bima Yojana
SLA	Service Level Agreement
SSA	Sarva Shiksha Abhiyaan

1 Introduction to Aadhaar Authentication Service

1.1 Service Definition

Aadhaar Authentication is defined as the process wherein, Aadhaar number along with the Aadhaar holder's personal identity information is submitted to the Central Identities Data Repository (CIDR) for matching following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it.

Prima facie, authentication qualifies as a service to be performed by UIDAI, as and when the National Identification Authority is setup under the Act of parliament. UIDAI shall offer Aadhaar-based authentication as a service that can be availed by government / public and private entities/agencies that wish to authenticate the identity of their customers / employees / other associates (based on the match of personal identity information) before providing them access to their services / business functions / premises, etc.

Some key features of Aadhaar authentication service are:

a) UIDAI shall offer Aadhaar-based authentication services free of charge till December 2013.

b) The use of Aadhaar-based authentication to enable their services / business functions is optional. Government / public / private entities use it only on a voluntary basis.

c) UIDAI encourages user entities to adopt federated authentication system, i.e., a combination of Aadhaar authentication and their own authentication systems. In case of user entities that already have their own authentication systems in place, Aadhaar authentication is envisaged to act in conjunction with existing authentication systems and strengthen the overall authentication rather than replace existing authentication systems.

d) UIDAI shall provide Aadhaar-based authentication services on a best-effort basis. UIDAI shall endeavour to inform and educate potential users of Aadhaar-based authentication and other key actors in the Aadhaar ecosystem of the benefits, risks and implications of using Aadhaar-based authentication. UIDAI is not liable for results of authentication to the agencies that use Aadhaar-based authentication to enable their services.

326

e) Aadhaar authentication services cannot be used for purposes that are anti-government, anti-State, illegal, discriminatory or related to money laundering.

1.2 Service Description

1.2.1 Introduction to the Service

Aadhaar-based authentication refers to the sequence of events during which the personal identity information / data of an Aadhaar-holder is matched with their personal identity information / data that is stored in the CIDR. An Aadhaar holder's Personal Identity Data (henceforth referred to as PID) includes his or her demographic details, one-time password (OTP with a limited validity period) sent to the Aadhaar holder's cell phone (stored in the CIDR) and the Aadhaar holder's biometric information (fingerprint and iris scan).

UIDAI, in its "Aadhaar Authentication Framework" document has listed the various authentication types that it offers. For each service that they wish to enable by Aadhaar authentication, user agencies choose an authentication type depending on their business requirements. The PID collected by the user entity for authentication is determined by the authentication type chosen.

This document addresses itself to the operating model for online[1] authentication of an Aadhaar holder's identity, i.e., where an Aadhaar holder's PID that is fed into the authentication device at the time of authentication are compared with the corresponding PID stored in UIDAI's Central Identity Data Repository (CIDR).

When an Aadhaar-holder claims their identity to seek access to a government or business service, proof of their identity is sought. The specific PID sought by the service provider is based on the authentication type of their choice. The collected PID is transmitted to CIDR which matches the received PID with the data existing at CIDR against the given Aadhaar number and determines whether the authentication is an *"accept"* or a *"reject"*. The result is communicated to the authentication device where the authentication request has originated. No Personal Identity Information (PII) is returned as part of the response.

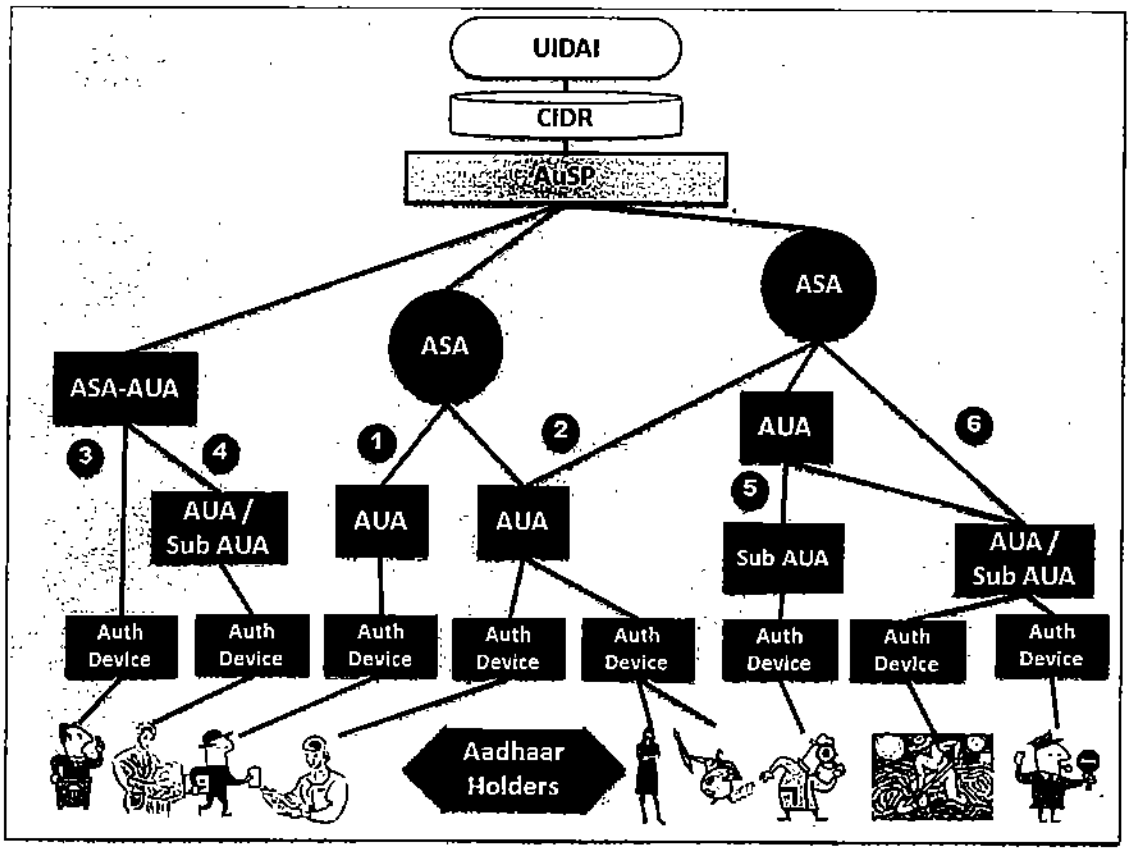
1.2.2 Introduction to Key Actors in Aadhaar authentication

The following figure identifies the key actors in the Aadhaar authentication model and depicts six possible scenarios in which the key actors could engage with each other. Brief description of key actors and the scenarios in which they engage with each other follow the figure. Detailed descriptions of key actors, their roles, responsibilities and

[1] Offline authentication is where the identity information collected at the time of authentication by the authentication device is compared to those stored elsewhere such as on a smartcard that is carried by the identity holder.

327

obligations of each actor and how they engage with each other in the Aadhaar authentication ecosystem follow in subsequent sections of this document.



1. **Unique Identification Authority of India (UIDAI):** UIDAI is the overall regulator and overseer of the Aadhaar authentication system. It also owns and manages, either by itself or through an agency, the Central Identities Data Repository (CIDR) that contains the personal identity information / data of all Aadhaar-holders. Presently UIDAI will manage the CIDR through a Managed Service Provider (MSP).

2. **Authentication Service Provider (AuSP):** AuSP is the entity that offers Aadhaar-based authentication services on behalf of UIDAI. To start with, the role of AuSP will be played by the entity that is the MSP. In the future, as authentication volumes go up, it is possible that more AuSPs are added to the authentication ecosystem.

3. **Authentication Service Agency (ASA):** ASAs are agencies that have established secure leased line connectivity with the CIDR compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies (see below for description of AUA) and transmit AUAs' authentication requests to CIDR. Only agencies contracted with UIDAI as ASAs shall send authentication requests to the CIDR; no other entity can directly communicate

with CIDR. An ASA could serve several AUAs; and may also offer value added services such as multi-party authentication, authorization and MIS reports to AUAs. Such value added services (over and beyond the basic Aadhaar authentication service) are not covered in this operating model. An ASA is bound to UIDAI through a formal contract.

4. **Authentication User Agency (AUA):** AUAs are agencies that uses Aadhaar authentication to enable its services and connects to the CIDR by itself (as an ASA) or through an existing third party ASA. It is also possible that an AUA engages more than one ASA. In order to directly connect to the CIDR, an AUA needs UIDAI's approval to become an ASA. An AUA could also transmit authentication requests from other entities that are "Sub AUAs" under it (see details on Sub AUA below). AUAs can also act as an aggregator offering authentication services to Sub-AUAs below them and may also offer value added services such as multi-party authentication, MIS reports and authorization to their Sub AUAs. An AUA enters into a formal contract with UIDAI in order to access Aadhaar authentication.

5. **Sub AUA:** An agency / entity (any legal entity registered in India) desiring to use Aadhaar authentication to enable its services could become an AUA or it could access Aadhaar authentication services through an existing AUA. In the latter case, it becomes a Sub AUA of the existing AUA which it engages. The following are some possible examples: (i) Government of any State/Union Territory could become an AUA and several ministries/departments in the State could access Aadhaar authentication services through the State government as its Sub AUAs. (ii) A small entity or business (e.g. a small scale bank) which does not want to directly engage in a formal contract with UIDAI but still wants to use Aadhaar Authentication, may choose to access Aadhaar services as a Sub AUA of an existing AUA (e.g. a large bank or any aggregator AUA offering AUA services). (iii) Several entities could combine under a single AUA for business reasons. Ex. Several hotels could access Aadhaar authentication as Sub AUAs of an Hoteliers Association that becomes an AUA. In all such cases UIDAI has no direct contractual relationship with the Sub AUA. Only the AUA is contracted to UIDAI and shall be responsible for all authentication requests flowing through it, including those originating from its Sub AUAs.

6. **Authentication Devices:** These are electronic actors that form a critical link in the Aadhaar authentication service. These are the devices that collect personal identity data (PID) from Aadhaar holders, prepare the information for transmission, transmit the authentication packets for authentication and receive the authentication results. They could be operator-assisted devices or self-operated devices. Examples of authentication devices include desktop PCs, laptops, kiosks,

handheld mobile devices, etc. They could be operated by the AUA (or the Sub AUA) or agents of AUA / Sub AUA.

7. **Aadhaar holders:** These are holders of valid Aadhaar numbers who seek to authenticate their identity towards gaining access to the services offered by the AUA or their Sub-AUAs.

The above figure also depicts six possible scenarios in which key actors in the Aadhaar authentication ecosystem could engage with each other (numbered 1-5 in the figure):

1. **Scenario-1:** In this scenario, entities that become an AUA choose to connect to the CIDR through any of the existing ASAs. Examples: (i) A government department (say Department of Civil Supplies) becomes an AUA and chooses to connect to the CIDR through an existing ASA, possibly a telecom carrier that has already established secure leased line connectivity to the CIDR. (ii) A bank becomes an AUA and chooses to connect to the CIDR through an existing ASA, possibly an organization such as National Payments Corporation of India (NPCI).

2. **Scenario-2:** This scenario refers to the case where an AUA chooses to engage multiple ASAs to connect to the CIDR. Possible reasons why AUAs may choose to do so include business continuity planning (to ensure continuous availability of Aadhaar authentications service even if one ASAs services fail) and accessing different value added services from different ASAs.

3. **Scenario-3:** An entity such as a large bank becomes an AUA and chooses to directly connect to the CIDR by establishing secure leased line connectivity to CIDR. In this case it is an AUA and is also its own ASA. Such entities can also offer ASA services to other AUAs (this case is described as Scenario-2).

4. **Scenario-4:** This is an extension of the earlier scenario. In this case, the ASA-AUA (such as a large bank) that establishes its own secure leased line connectivity to the CIDR serves other AUAs / Sub AUAs (such as other smaller banks that choose to engage an ASA rather than establish their own leased line connectivity to the CIDR). The latter entity could connect to the ASA-AUA as an AUA (in which case it is directly contracted to UIDAI) or as a Sub AUA of the ASA-AUA.

5. **Scenario-5:** Some entities desiring to use Aadhaar authentication may choose to route their requests through an existing AUA rather than becomes AUAs themselves. In such cases, they become Sub AUAs of existing AUAs. Possible examples have been provided earlier in this section.

6. **Scenario-6:** Some AUAs may choose to transmit some of their Aadhaar authentication requests through an ASA and the remaining through another AUA.

330

This could happen when the latter AUA provides value added services that the former AUA desires to access (such as providing reconciliation services to banks in funds transfer transactions). A possible example: a bank could go through its ASA for services such as balance inquiry and go through a large bank for services such as funds transfer. In such cases, the bank plays the role of an AUA when going through an ASA and at the same time is a Sub AUA of another AUA (the larger bank) when going through the larger bank.

More details regarding key actors, their roles, responsibilities and obligations and how they engage with other actors in Aadhaar authentication ecosystem are addressed in Sections 2 and 3.

1.2.3 Federated mode of Aadhaar authentication service

UIDAI offers Aadhaar authentication that can be used alone or in conjunction with AUAs/Sub-AUAs domain/application specific authentication scheme (called "federated authentication"). For example, in federated authentication, a Bank could choose to use an ATM card and fingerprint for authentication of which the ATM card is authenticated within Bank's application whereas the fingerprint is authenticated against data in the CIDR using Aadhaar authentication.

Most current authentication systems could be described as "local" (i.e., pertaining to and/or valid for a few services, situations or entities) and "revocable" (wherein an existing identity factor could be revoked and reissued as a result of expiry, compromise or other valid reasons). Such revocable, local authentication systems come with a set of strengths and limitations. Aadhaar authentication system, on the other hand, could be described as "global" (because of its applicability across situations, AUAs and services) and "non-revocable" (because Aadhaar identity factors such as fingerprints and iris scans cannot usually be revoked/replaced). Global, non-revocable/permanent authentication systems come with their own set of strengths and limitations.

In the federated authentication model, the global-irrevocable Aadhaar authentication co-exists with and strengthens the local-revocable authentication of AUAs. It is expected that such a federated approach would result in authentication systems that are stronger and more reliable than those that are based either only on global-irrevocable model or only on local-revocable model.

Aadhaar authentication should not be considered as a replacement for existing authentication systems, rather a complimentary scheme. UIDAI encourages complimentary authentication frameworks that may be specific to a domain/application, to take advantage of Aadhaar as a global identity system. For example, an online identity provider (as an AUA) may use Aadhaar and provide User ID

and password based authentication for Internet applications. In that case, that AUA uses Aadhaar authentication while creating initial User ID and password and then allows residents to use that User ID and password for logging into various Internet applications. When there are no local authentication schemes, AUAs/Sub-AUAs may use Aadhaar authentication 'as-is' and still gain great value in strongly identifying their customers/ beneficiaries.

The following are some types of situations where an AUA or a Sub-AUA could use Aadhaar authentication:

1. **One time usage:** When enrolling a new customer or creating a new service account for an individual. Examples are the issuance of a new PAN card, a new passport, creation of a new bank account or an internet service account for an online business. The AUAs in all such cases could authenticate an applicant's identity using the applicant's Aadhaar PID before issuing their own authentication factors.
2. **Periodic usage:** AUAs can also use Aadhaar based authentication system for periodic update of their customers' (or employees' or associates') identity information. Examples are using Aadhaar authentication as a basis for renewing an Aadhaar holder's KYC data, the address of a bank account holder, etc.
3. **Regular transactional usage:** AUAs/Sub AUAs can also use Aadhaar authentication system for carrying out any of their business transactions. Examples include banks that authenticate a customer's Aadhaar PID as well as bank-related identity information (account number/user id along with password/OTP, etc.) before enabling banking transactions such as funds transfer, funds withdrawal, etc.

Aadhaar authentication must therefore be viewed as a way to strengthen AUAs'/ Sub AUAs' existing authentication systems, rather than as a replacement for AUAs' existing authentication systems. While the federated model does not mandate the existence or use of an AUA's own authentication (if an AUA/ Sub-AUA so wishes, they could use only Aadhaar authentication by itself), AUAs/ Sub-AUA are encouraged to use Aadhaar authentication in conjunction with their own local authentication to render the overall authentication system stronger and more reliable.

2 Engagement Model: Roles, Responsibilities and Obligations of Key Actors

The following key actors in the Aadhaar authentication ecosystem will be studied in detail in this section. For each of the key actors, this section identifies their role, how they enter the Aadhaar authentication ecosystem, and their key responsibilities and obligations.

1. UIDAI
2. Authentication Service Provider (AuSP)
3. Authentication Service Agency (ASA)
4. Authentication User Agency (AUA)
   a. Sub AUA
   b. Authentication Device (AD)
5. Aadhaar holder

2.1 Unique Identification Authority of India (UIDAI)

2.1.1 Role of UIDAI

Unique Identification Authority of India (UIDAI) has been created with the mandate of providing a Unique Identity (Aadhaar) to eligible applicants, and also defining the usages and applicability of Aadhaar for the delivery of various services. UIDAI offers online authentication of Aadhaar holders' identity, a service that can be used by government / public / private agencies to enable their services / business functions that require establishing of the identity of their customers / employers / associates.

UIDAI is also the overall overseer and regulator of the Aadhaar-based authentication ecosystem.

2.1.2 Responsibilities and Obligations of UIDAI

i. UIDAI issues Aadhaar number to eligible applicants.

ii. UIDAI is the custodian of all issued Aadhaar numbers and their corresponding Aadhaar-based Personal Identity Data / Information (PID/PII).

iii. UIDAI provides update services and other related lifecycle services to residents for managing their PID within CIDR.

iv. UIDAI provides Aadhaar-based authentication services to AUAs that wish to use Aadhaar Authentication for establishing identity of Aadhaar holders before providing access to their services.

v. UIDAI determines the operating and engagement model for Aadhaar-based authentication.

vi. UIDAI shall determine the rules regarding the usage of Aadhaar number and Aadhaar authentication.

vii. UIDAI determines the eligibility criteria for ASA, facilitates the application and registration of ASAs and enters into contracts with ASAs.

viii. UIDAI determines the eligibility criteria and entry process for AUA, facilitates the application and registration of AUAs and enters into contracts with AUAs.

ix. UIDAI determines standards and specifications that will be adhered to by all those participating in the Aadhaar authentication ecosystem (including ASA, AUA and Sub AUA). The standards and specifications include systems and processes, API specifications, infrastructure specifications (including device specifications), process specifications, technology specifications, certification specifications (if any), audit specifications, security specifications and SLAs (service level agreements) where applicable. In summary, UIDAI shall determine minimum standards and specifications for Aadhaar authentication and ecosystem partners may extend and add further specifications and standards to meet their domain and application needs. Please refer to documents published on UIDAI's website for the standards and specifications prescribed by UIDAI. UIDAI may choose to certify all applications that will be used by AUAs (and Sub AUAs) in enabling their Aadhaar authentication operations. This would include:

   - Certification (by itself or through approved independent certification agencies) of applications (such as applications driving the authentication systems and applications in the AUAs' systems) that will be used by AUAs and other participants in their Aadhaar authentication systems.

   - Certifying fingerprint and iris sensor and extractor pairs that will be incorporated in authentication devices. It is the responsibility of vendors of sensor and extractor pairs to get their products certified by Standardisation Testing and Quality Certification (STQC) Directorate and for using the same in their devices

x. UIDAI reserves the right to conduct audits of all key actors in the authentication ecosystem including ASA and AUA – either by itself or through UIDAI-appointed/approved independent audit agencies to examine compliance to its standards and specifications. As part of these audits, UIDAI/audit agency could

334

inspect the premises, operations and systems, infrastructure, security, etc. of the audited entity.

xi. UIDAI retains the right to take appropriate action against parties not complying with UIDAI's specifications including disqualification to use Aadhaar authentication system / termination of contract with UIDAI after appropriate grace period for remedial action as provided in the respective contracts.

xii. UIDAI shall provide a framework for the Dispute Resolution Mechanism for the Aadhaar authentication ecosystem.

xiii. In the future if any charges are associated with Aadhaar authentication, UIDAI could determine the charges or determine the framework to determine charges.

xiv. UIDAI will play any role when necessary to ensure that the system continues to offer uninterrupted services and run successfully.

2.2 Authentication Service Provider (AuSP)

2.2.1 Role of AuSP

a) Authentication Service Provider (AuSP) is responsible for the provisioning of Aadhaar authentication services on UIDAI's behalf.

b) AuSP's main areas of responsibility include authentication transaction operations (i.e., receive authentication request, execute a match of PID received with the identity information on CIDR and transmit the result), network operations, data centre operations, availability of authentication service, SLAs with AUA if any and monitoring operations & performance metrics.

2.2.2 How AuSP enters the Aadhaar Authentication ecosystem

a) To start with, when the authentication volumes are expected to be low, the role of AuSP will be played by the Managed Service Provider (MSP). In future, as authentication volumes increase, it is envisaged that more entities will play the role of AuSP.

b) At that time, UIDAI will determine the process of adding more AuSPs to the Aadhaar authentication ecosystem; and manage the process to bring in more AuSPs.

2.3 Authentication Service Agency (ASA)

2.3.1 Role of ASA

a) ASA is an agency that has established secure leased line connectivity to the CIDR to transmit authentication request on behalf of AUAs and receive response back from CIDR. ASAs build and maintain their secure connectivity to CIDR in compliance with the standards and specifications set by UIDAI. Examples of ASAs are:

   i. A government department such as a State's IT Department could become an ASA and establish a secure UIDAI-compliant leased line connectivity to CIDR through which several ministries/departments in the State could channel their authentication requests.

   ii. A telecom carrier that obtains UIDAI's approval could establish a secure leased line connection with the CIDR and offer ASA services to AUAs.

   iii. An organization such as National Payments Corporation of India (NPCI) could establish a secure UIDAI-compliant leased line connectivity to CIDR and offer authentication services and possibly value added services to banks.

b) ASAs receive Aadhaar authentication request from AUAs and transmit the same to CIDR. In turn they receive CIDR's response that they transmit back to the AUA that has placed the authentication request.

c) An ASA could serve more than one AUA.

d) It is conceivable that some ASAs offer value added services to AUAs in addition to providing them with connectivity to CIDR. Examples of value added services include authorization services, MIS and funds reconciliation (in case of banking). However, such arrangements over and beyond basic Aadhaar authentication service that an ASA and an AUA may enter into are not the concern of UIDAI and are out of the scope of this document.

2.3.2 How ASAs enter Aadhaar Authentication ecosystem

a) The eligibility criteria for an agency to be considered for engagement as an ASA are as under:

A. The agency should either be

i. A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government

OR

ii. An Authority constituted under the Central / State Act

OR

iii. A Not-for-profit company / Special Purpose organization of national importance

OR

iv. A company registered in India under the Indian Companies Act 1956 meeting the following requirements:

a. Financial capabilities – An annual turnover of at least Rs. 100 crores in last three financial years, and

b. Technical capabilities:

A Telecom Service Provider (TSP) operating pan India fibre optics network and should have a minimum of 100 MPLS Points of Presence (PoP) across all states

OR

Should be a Network Service Provider (NSP) capable of providing network connectivity for data, voice transmission and should have an agreement with the TSP having 100 MPLS PoPs

OR

System Integrator having necessary arrangement with TSP/NSP as described above

c. The agency should not have been blacklisted by Central / State Governments / PSUs of Central / State Governments in the last five years

B. The agency should give an undertaking and demonstrate the capability of design, configure, implement and maintain the infrastructure and systems required for an ASA as per UIDAI's specifications and certify that necessary human resources with requisite skills are in place to perform the functions required as an ASA.

The decision of UIDAI regarding engagement of ASA shall be final.

b) ASAs enter Aadhaar authentication ecosystem through UIDAI's ASA appointment process determined and conducted by UIDAI.

c) Entities wishing to act as ASA apply to UIDAI providing necessary information along with supporting documents where relevant. UIDAI shall examine the applications and approve qualifying applicants as ASA. Approved ASAs enter into a contract with UIDAI and are permitted to build secure leased line connections to the CIDR that comply with UIDAI's standards and specifications.

d) It is envisaged that UIDAI's ASA appointment process is open and continuous, i.e., applicants could file in their applications any time and could be appointed if they qualify. However, UIDAI could change this policy at a later point.

e) Each ASA contract is for a specified duration at the end of which an ASA is free to apply for a renewal. UIDAI shall evaluate the renewal application and approve renewals for qualifying applications.

2.3.3 Responsibilities and Obligations of ASA

i. ASAs shall adhere to their contract with UIDAI in complying with UIDAI's standards and specifications including SLAs if relevant.

ii. The ASA shall ensure that all their infrastructure and operations including systems, processes, IT and biometric infrastructure, security, etc., are compliant with UIDAI's standards and specifications.

iii. When an ASA receives an authentication request from an AUA, it is recommended that the ASA performs basic checks on the authentication input before forwarding it to CIDR. The authentication request is forwarded to CIDR only if it is compliant and complete. Else, it is returned to the AUA with appropriate error message (who then forwards it to the authentication device with necessary instructions).

iv. On receiving the response from CIDR, ASA transmits the result of the transaction to AUA that has placed the request.

v. It is highly recommended that the ASA maintains logs of all authentication transactions it processes. These logs shall be retained for specified duration determined by UIDAI and shall be shared with other entities only on need-basis. These logs shall capture transaction details such as Aadhaar number, requesting AUA, timestamp, etc. but not PID associated with an authentication transaction. The storage of transaction logs shall comply with the applicable laws of the country like the IT Act 2000 etc.

vi. In conducting their operations, the ASA shall comply with all applicable laws and regulations in the country in the areas of data security and management like IT Act 2000.

vii. The ASAs shall ensure that its systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body before commencement of its operations and the ASA shall provide a certified audit report, to UIDAI, confirming its compliance with the standards, directions, specifications, etc. issued by UIDAI, in this regard, from time to time.

viii. The ASAs shall ensure that its operations and systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body on an annual basis and the ASA shall provide a certified audit report, to UIDAI, confirming its compliance with the standards, directions, specifications, etc. issued by UIDAI, in this regard, from time to time.

In addition to this, UIDAI reserves the right to audit ASAs by itself or through agencies appointed / approved by UIDAI. During these audits, the ASA shall cooperate fully with UIDAI / audit agency and provide access to their premises, procedures, records, systems, personnel and any other relevant part of their authentication operations. In case of non-compliance, UIDAI could take appropriate action (such as termination of contract after appropriate grace period for remedial action). The cost of the audits is borne by the ASA.

ix. The ASA shall keep UIDAI informed of the list of AUAs it serves. On entering into a contract with a new AUA, the ASA informs UIDAI (along with the details sought by UIDAI) before commencing service to the new AUA. Similarly when an ASA disengages with an AUA, the ASA shall inform UIDAI within 7 days of the disengagement.

x. The ASA may have a contract with the AU A and may provide any value added services to the AUA as part of that contract. However, such value added services do not form part of Aadhaar Authentication.

xi. The ASA shall be responsible to UIDAI for all their authentication related operations (as covered in the contract between UIDAI and the ASA). Even if the ASA outsources parts of its operations to other entities, the responsibility for the operations and results of authentication related operations lies with the ASA.

xii. In case of investigations around authentication related fraud or dispute, the ASA shall extent full cooperation to UIDAI (or their agency) and/or any other authorized investigation agency. This includes providing access to their premises, records, systems, personnel, infrastructure, any other relevant resource / information and any other relevant aspect of its authentication operations.

340

2.4 Authentication User Agency (AUA)

a) AUA is any agency that seeks to use Aadhaar authentication to enable its services. Each AUA can use Aadhaar authentication to enable one or more of its services. The AUA chooses an appropriate authentication type for each of the services enabled by Aadhaar authentication. An AUA has the option of connecting to the CIDR by itself or through an existing ASA.

b) Examples of AUA:

   a. Department of Civil Supplies, which seeks to authenticate a target resident before issuing them their monthly ration of rice, kerosene, etc.

   b. A bank that seeks to authenticate its customers before letting them complete a financial transaction such as withdrawal or transfer of funds. Such transactions could be operator-assisted (when they take place in the bank's premises) or self-operated (as in internet banking).

   c. The administration/security department of a high-security building/zone that seeks to authenticate individuals seeking entry into the building/zone.

   d. A social networking site/ e-commerce website that seeks to authenticate customers/ subscribers during the registration process

2.4.1 Role of AUA

a) The AUA is the principal entity that drives authentication requests to enable their services. An AUA can use Aadhaar authentication to enable one or more of their services. Based on the result of the authentication, the AUA determines whether or not to provide Aadhaar-holders access to their services.

b) An AUA could send its authentication requests directly to CIDR (in which case it needs UIDAI's approval to become an ASA) or engage an existing ASA for transmitting its authentication requests. An AUA could also engage more than one ASA if they wish to.

c) The AUA shall ensure that the authentication request originating at an authentication device is compliant with the standards and specifications prescribed by UIDAI (refer Appendix I) and complete before transmitting the request to its ASA. After the AUA receives the result of the authentication from CIDR, it determines whether or not to provide service to the Aadhaar-holder; and it transmits the authentication result to the originating authentication device along with instructions on the next steps.

d) It is also possible for AUAs to transmit authentication requests originating from Sub AUAs under it. Sub AUAs are entities that wish to use Aadhaar authentication to enable their services, but choose to connect to the CIDR through an existing AUA rather become AUAs themselves. Details about Sub AUAs can be found in Section 2.5.

2.4.2 How an AUA enters the Aadhaar Authentication ecosystem

a) The agency should either be:

i. A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government

OR

ii. An Authority constituted under the Central / State Act

OR

iii. A Not-for-profit company / Special Purpose organization of national importance

OR

iv. A bank / financial institution / telecom company

OR

v. A legal entity registered in India that seeks to use Aadhaar authentication to enable its services. Applications from such agencies would be considered and approved by AUA Approval Board to be constituted by UIDAI.

The agency should give an undertaking and demonstrate the capability to implement and maintain the infrastructure and systems required to become an AUA.

The decision of UIDAI regarding engagement of AUA shall be final.

b) Agencies seeking to use Aadhaar-based authentication to enable their services shall apply to UIDAI by providing necessary information along with the required supporting documentation as well as the information on the ASA through which the AUA shall connect to the CIDR.

c) On receipt of necessary information (and documentation if relevant), UIDAI approves an AUA. On approval, the AUA and UIDAI enter into a contract. As long as the role of AuSP is played by the MSP, AUA need not enter into a contract with the AuSP. However, if more players start playing the role of AuSP, AUAs might

have to enter into contracts with one/more AuSP (on issues such as authentication SLAs) before they can start availing Aadhaar authentication services.

2.4.3 Responsibilities and Obligations of AUA

i. For each service for which they would like to use Aadhaar authentication, the AUA chooses an appropriate authentication type and shall inform UIDAI regarding the same. The choice of authentication type in turn, indicates the specific identity information to be sought from the Aadhaar-holder to enable that service. Details of authentication types offered by UIDAI can be found in the "Aadhaar Authentication Framework" document. The choice of authentication type for a service is a decision of the AUA alone; and none of the other entities including UIDAI and ASA are responsible for this decision. It is possible for an AUA to change the authentication type of any service if it so desires, under intimation to UIDAI.

ii. The AUA shall adhere to the processes and the AUA on-boarding checklist provided by UIDAI for getting started with Aadhaar authentication service. As and when there are any changes in the parameters, the AUA shall keep UIDAI informed of the list of its services that are enabled by Aadhaar authentication. This process is expected to be done, possibly in a self-service mode (such as an online update through UIDAI portal).

iii. The AUA shall establish its authentication related operations (including systems, processes, technology, infrastructure, security, etc.) in compliance with UIDAI's standards and specifications.

iv. AUA shall be responsible for provisioning of network from authentication devices to the AUA server and between the AUA server and the ASA server, and shall ensure compliance to UIDAI's security specifications. In addition, they shall be responsible for procuring and deploying any hardware/software/certificate/etc. for complying with Aadhaar authentication standards.

v. AUA shall ensure that devices used for Aadhaar authentication are procured, deployed, and managed by them or their agent(s) in compliance with UIDAI specifications and standards published by UIDAI from time to time.

vi. The AUA shall log all its authentication transactions and maintain them for a specified period of time. The logs shall capture details of an authentication transaction but not corresponding PID. The storage of transaction logs shall

comply with applicable laws and regulations of the country like the IT Act 2000 etc. The details of logs stored, the duration of storage and any other aspect of data storage shall be determined by UIDAI specifications, regulations applicable to the AUA's service and industry, the AUA's own requirements and other applicable laws and regulations.

vii. It is highly recommended that the AUA shall deploy as part of its systems, a Fraud Analytics module that is capable of analysing authentication related transactions to identify fraud cases and patterns. If the AUA is a victim of a fraud or identifies a fraud pattern through its fraud analytics system, it shall share all necessary details of the fraud with UIDAI.

viii. The encrypted PID block should not be stored, unless it is for buffered authentication for a short period of time, and after transmission, it should be deleted. Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database. The AUA shall ensure that all relevant laws and regulations are adhered to in relation to data storage and data protection (with regard to Aadhaar-based identity data) in their systems, that of their agents (if applicable) and with authentication devices.

ix. In cases where the authentication devices are operated by AUA's personnel (or personnel of their agents), the AUA is responsible for ensuring that the operating personnel who are adequately trained to conduct Aadhaar-based authentication.

x. The AUA shall ensure that its systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body before commencement of its operations and the AUA shall provide a certified audit report, to UIDAI, confirming its compliance with the standards, directions, specifications, etc. issued by UIDAI, in this regard, from time to time.

xi. The AUA shall ensure that its operations and systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body on an annual basis to ensure compliance with UIDAI standards and specifications and the audit report should be shared with UIDAI upon request. It is the AUA's responsibility to ensure that their Sub AUAs and agents are also regularly audited.

In addition, UIDAI reserves the right to audit the AUA's operations and systems (and their agents if applicable), by itself or through an auditor appointed by UIDAI. During these audits, the AUA shall cooperate fully with the audit agency and provide them necessary access to their premises, procedures, records,

systems, personnel and any other relevant aspect of authentication operations. In case of non-compliance, UIDAI could take appropriate action (such as termination of AUA contract after suitable grace period for remedial action). The cost of these audits shall be borne by the AUA.

xii. The AUA is responsible for identifying exception-handling mechanisms and back-up identity authentication mechanisms when Aadhaar-based federated authentication fails. Authentication failures could occur due to process failures, infrastructure failures (including power, IT infrastructure, authentication devices, network connectivity) or biometric failures (where Aadhaar holder's biometric cannot be acquired or used for some reason).

xiii. When an AUA associates with a Sub AUA (details of Sub AUA in Section 2.5), the AUA shall inform UIDAI of the engagement before starting to serve the new Sub AUA. Similarly, when a Sub AUA disengages with the AUA, the AUA shall inform UIDAI within 7 days (or a period specified by UIDAI) of disengagement. The process of such updates is envisaged to be in a self-service mode (such as an online update through UIDAI portal). When an AUA engages with a Sub AUA, it generates a Sub AUA Code to identify the specific Sub AUA. When informing UIDAI of its engagement with the Sub AUA, the AUA also informs UIDAI of the new Sub AUA Code. When transmitting authentication requests from a Sub AUA, the AUA always includes the Sub AUA Code so that Aadhaar authentication transaction logs can track the origin of all authentication requests. It is necessary that for each Sub-AUA, a separate license key is used so that the engagement and disengagement of Sub-AUAs can be easily accomplished by creating and revoking their respective license keys.

xiv. It is the AUA's responsibility to ensure that all Sub AUAs under it are regularly audited for compliance with UIDAI specifications. In case of non-compliance or default, the AUA shall report the same to UIDAI and take correction action according to UIDAI's guidelines.

xv. When an AUA engages a Sub AUA, from UIDAI's perspective, the AUA is responsible for the connectivity between the Sub AUA's authentication devices to the AUA's systems.

xvi. Even if the AUA outsources parts of its operations to 3rd party entities, the responsibility for the authentication operations and results lies with the AUA. The AUA is also responsible for ensuring that the authentication related operations of such 3rd party entities comply with UIDAI standards and

345

specifications and that they are regularly audited by approved independent audit agencies.

xvii. In case of investigations around authentication related fraud or dispute, the AUA shall extend full cooperation to UIDAI (or their agency) and/or any other authorized investigation agency. This includes providing access to their (and if applicable their agents') premises, records, personnel, systems, relevant resource / information and any other relevant aspect of authentication operations.

xviii. An AUA shall proactively inform UIDAI of any misuse of Aadhaar data, authentication services, or any compromise of Aadhaar related data or systems within their network.

2.5 Sub AUA

a) Sub AUAs are agencies that access Aadhaar authentication through an existing AUA.

b) An entity desiring to use Aadhaar authentication could choose to become an AUA or it could choose to access Aadhaar authentication services through an existing AUA. In the latter case, it becomes a sub AUA of the existing AUA which it engages.

c) Possible examples:

   a. Nodal department such as the IT Department/ e-Governance Department of any State/Union Territory could become an AUA and several ministries/departments in the State could access Aadhaar authentication services through the Nodal department as Sub AUAs.

   b. Several entities, conceivably in similar business, could combine under a single AUA for business reasons. Ex. Several hotels could access Aadhaar authentication as Sub AUAs of a Hoteliers' Association that becomes an AUA

   c. Entities that have infrequent Aadhaar authentication requirements may choose to access Aadhaar services as Sub AUAs of existing AUAs.

2.5.1 Role of Sub AUA

a) A Sub AUA is similar to an AUA in its usage of Aadhaar authentication. The primary difference is that an AUA is contracted directly to UIDAI whereas a Sub AUA enters into a contract with the AUA it engages.

b) A Sub AUA can use Aadhaar authentication to enable one or more of their services. Based on the result of the authentication, the Sub AUA determines whether or not to provide Aadhaar-holders access to their services.

2.5.2 How a Sub AUA enters the Aadhaar authentication ecosystem

a) An entity desiring to become a Sub AUA identifies the AUA to engage with and applies to the AUA by providing necessary information and supporting documentation if necessary.

b) The Sub AUA commits to compliance with UIDAI standards and specifications in their Aadhaar authentication operations.

c) The AUA informs UIDAI of the engagement with the Sub AUA and commences its services to the Sub AUA.

2.5.3 Responsibilities and Obligations of Sub AUAs

The responsibilities of a Sub AUA will be similar to that of an AUA. The responsibilities and obligations of an AUA covered in Section 2.4.3 will be applicable to Sub AUA as well.

2.6 Authentication Devices

Authentication devices are electronic actors in the Aadhaar authentication system where an Aadhaar authentication transaction is initiated. These could be operator-assisted or self-operated devices. Examples of authentication devices include desktop PCs, laptops, kiosks and handheld mobile devices that are, if required, integrated with / connected to biometric devices (for capturing fingerprints and/or iris scans).

2.6.1 Role of Authentication Devices

Aadhaar authentication is initiated through authentication devices. Authentication devices are deployed to perform the following key functions:

a) Collect PID from Aadhaar holders.

b) Perform basic checks on the information collected for completeness and compliance.

c) Prepare the authentication data packet for transmission.

d) Transmit the authentication packets for authentication.

e) Receive the authentication results along with instructions for next steps if any.

2.6.2 How Authentication Devices are deployed in the Aadhaar authentication ecosystem

a) Authentication devices could be deployed in the Aadhaar authentication ecosystem by the AUA, Sub AUA or the agents of AUA/Sub AUA.

b) AUAs/ Sub AUAs shall be responsible for provision of network from devices to AUA/ Sub AUA server and to AUA/ ASA server and ensuring security. In addition, they shall be responsible for procuring and deploying any hardware/software/certificate/etc. for complying with Aadhaar authentication standards.

2.6.3 Features of Authentication Devices

i. They are compliant with UIDAI standards and specifications

ii. Authentication devices could be operator-assisted or self-operated.

iii. They must be capable of collecting relevant information from Aadhaar holders, prepare authentication data packets (PID block), performs structural validation of data, transmit data packets and receive authentication results along with instructions on next steps if any. Collection of Aadhaar information by the authentication devices shall be carried out in compliance with UIDAI specifications.

iv. Authentication devices must be deployed such that they cannot retain Aadhaar holders' biometric and OTP data captured for the purposes of Aadhaar authentication during an transaction (except in case of *Buffered Authentication* described in Section 3.1, in which case they will be able to store encrypted data for a certain period of time).

v. In terms of data storage, authentication devices must comply with all applicable laws and regulations of the country like IT Act 2000, etc.

2.7 Aadhaar Holder

A holder of Aadhaar-based identity (Aadhaar-holder) is any eligible individual who has enrolled with UIDAI and obtained their unique Aadhaar number. In the context of Aadhaar authentication, they are usually associated with AUAs (or Sub AUAs) as customers, employees or associates; and in this capacity, seek access to AUAs' / Sub AUAs' services.

2.7.1 Role of Aadhaar-Holder

a) Aadhaar-holders are the owners of their PID stored in the CIDR. They are generally associated with AUA / Sub-AUA as customers/ beneficiaries/employees/ associates, etc. and seek access to the AUA's / Sub AUA's services. In order for them to gain access to these services, their identity is authenticated using their Aadhaar-based identity information (and AUA / Sub AUA-based identity information where relevant).

b) Depending on the authentication type sought by AUA/Sub AUA, they provide their Aadhaar-related demographic and/or biometric identity information before they are provided access to the service they are seeking.

c) They enjoy rights and privileges and are subject to obligations as identified in the "Aadhaar Holders' Charter" of Aadhaar-based authentication service.

d) *Examples:*

a. An individual who goes to a fair price shop to get her monthly ration of rice.

b. A bank account holder who goes to a bank where she holds an account to conduct a financial transaction such as withdrawal or transfer of funds; or a bank account holder who wishes to complete a financial transaction through internet banking from her home computer.

c. An individual who has to produce proof of identity while applying for a new telephone connection.

2.7.2 How Aadhaar-holders enter the Aadhaar Authentication ecosystem

a) Eligible individuals seeking Aadhaar identity enter the Aadhaar ecosystem when they enrol with one of the UIDAI-approved registrars by providing their demographic and biometric identity information.

b) Upon successful completion of the enrolment process, each eligible individual obtains his or her unique Aadhaar number. The demographic and biometric identity information of each Aadhaar-holder is stored against the corresponding Aadhaar number in the CIDR.

2.7.3 Responsibilities and Obligations of Aadhaar-Holder

i. Aadhaar-holders shall provide their consent to provide and to be authenticated using their Aadhaar-based PID sought by the AUA / Sub AUA and shall provide the Aadhaar based PID voluntarily in order to gain access to the AUA's / Sub AUA's services they wish to access.

ii. It is the Aadhaar-holders' responsibility to keep their PID in the CIDR valid and current. They do so on a periodic-basis or on a need-basis as the case may be. Some instances where an update may be necessary:

a. Informing UIDAI of a change in address

b. Updating the collection of fingerprints on a periodic basis

c. Correction of any errors

350

iii. Aadhaar holders shall approach UIDAI in case they have reason to believe that their Aadhaar PID has been compromised by any of the actors in the authentication ecosystem.

iv. Aadhaar holders shall proactively inform UIDAI of any misuse of Aadhaar data or authentication services.

v. Their rights, responsibilities are obligations are covered in detail in the Aadhaar Holders' Charter.

3 Variation of the Engagement Model: Buffered Authentication

There may be cases where the authentication model described above undergoes minor variations. One such case is Buffered Authentication.

a) In some situations, it is envisaged that the AUA will not be seeking real-time authentication from CIDR. Possible examples include:

   a. When connectivity is not available or possible at the point of PID collection preventing real-time transmission of authentication requests.

   b. When the nature of AUA's service does not require real time authentication or is not suitable for real time authentication (as when a very high number of authentications have to be completed within a short duration and the AUA's service can do without real time authentication. Ex. attendance tracking scenario).

b) In such cases, PID of multiple Aadhaar-holders are collected and buffered at the authentication device; and transmitted at a later time. This is referred to as *Buffered Authentication.*

c) The Buffered Authentication process therefore varies slightly from that of the normal case till the authentication requests are transmitted from the authentication device. From this point, the model and process is similar to the normal scenario – the buffered set of authentication requests are checked by the AUA and transmitted to ASA, who further performs structural validation of data and forwards to the AuSP; upon receiving the authentication result for each request, the ASA forwards them to the AUA who forwards the same to the authentication device that has placed the requests.

d) Even though the authentication device may transmit multiple authentication requests at the same time, each authentication request will be treated as a separate transaction in the Aadhaar authentication system and each authentication request will have its own *Auth code.*

e) It is the AUA's responsibility to ensure that the authentication devices being used are capable of managing Buffered Authentication (which may include capability to store multiple authentication requests, transmit them at the same time, and receive and store results of multiple authentications; and necessary security features).

f) There will be an upper limit for the duration of time that authentication requests can be buffered. This duration will be determined by UIDAI specifications.

g) Since Buffered Authentication is provided only for supporting occasional connectivity issues on the field, buffering of authentication requests should be done *only* on authentication devices and not on the servers of Sub AUA / AUA / ASA.

353

सत्यमेव जयते

Aadhaar
Authentication Implementation Model

UIDAI – AUA Agreement

Version 3.3

AADHAAR

Unique Identification Authority of India
(UIDAI)

 354

AUTHENTICATION USER AGENCY AGREEMENT

This **AUTHENTICATION USER AGENCY AGREEMENT** ("**Agreement**") is made as of this _____ day of _____, and year _____, by and between:

1. **UNIQUE IDENTIFICATION AUTHORITY OF INDIA**, an authority set up by the Planning Commission, Government of India, vide Notification dated 28 January, 2009, having its address at 3rd Floor, Tower II, Jeevan Bharati Building, Connaught Circus, New Delhi-110001 (hereinafter referred to as "**UIDAI**", which expression shall unless repugnant to the context or meaning thereof, include its successors and permitted assigns), OF THE FIRST PART.

AND

2. _____
_____, having its address at _____
_____
_____
(hereinafter referred to as "**Authentication User Agency**", which expression shall unless repugnant to the context or meaning thereof, include its successors and permitted assigns), OF THE SECOND PART.

355

WHEREAS:

A. UIDAI has been set up with the mandate of issuing unique identification numbers, i.e., "Aadhaar Numbers" to the residents of India, based on their biometric and demographic information.

B. The Aadhaar Number and Personal Identity Information (PID) of the Aadhaar Holder can be authenticated through an online mechanism provided by UIDAI for this purpose, which authentication mechanism is provided by UIDAI free of charge till December 2013, where after the same may or may not be charged for, at the sole discretion of UIDAI.

C. The Authentication User Agency is desirous of using the Aadhaar Authentication Services provided by UIDAI, through an Authentication Service Agency, so as to provide Aadhaar Enabled Services to its beneficiaries, clients and customers and has approached UIDAI, by way of an application, for appointment as an Authentication User Agency.

D. The Authentication User Agency is aware of, and understands, the fact that UIDAI's operation of the Aadhaar Authentication Services is subject to limitations posed by technology, and UIDAI does not represent and warrant the same to be defect free.

E. The Authentication User Agency is aware of, and understands that the Aadhaar Authentication Services are provided on an 'as is' basis, without any express or implied warranties in respect thereof, and UIDAI does not assume any responsibility or liability for any damage, whether direct, indirect, incidental or consequential, arising as a result of the use of the Aadhaar Authentication Services except the damages which solely arise out of False acceptance by UIDAI biometric authentication services.

F. UIDAI has evaluated the application of the Authentication User Agency and has granted recognition to and approval for appointment of the Authentication User Agency as an Authentication User Agency for providing Aadhaar Enabled Services.

G. UIDAI has further evaluated the application of the Authentication User Agency and has granted recognition to and approval for appointment/empanelment of the Authentication User Agency as a KYC User Agency (KUA) for the e-KYC service, subject to annexure 1 duly signed by UIDAI and the Authentication User Agency. In such a case

Authentication User Agency is also referred to as KYC User Agency (KUA) and references to Authentication User Agency also mean KYC User Agency and similarly Authentication Service Agency also mean KYC Service Agency.

NOW THEREFORE, in consideration of the mutual covenants and promises set forth herein and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby covenant and agree and this Agreement witnesseth as follows:

1. DEFINITIONS & INTERPRETATION

"**Aadhaar Authentication Services**" shall mean the authentication services provided by UIDAI and used by Authentication User Agency where the personal identity information of/data of an Aadhaar-holder (who is a beneficiary, customer, employee or associate of the Authentication User Agency is matched with their personal identity information/data that is stored in the UIDAI's Central Identity Data Repository in order to provide Aadhaar enabled services to such Aadhaar holder. The Authentication User Agency shall avail Aadhaar authentication service by establishing a connection with UIDAI's Central Identity Data Repository, through an Authentication Service Agency The Aadhaar authentication services shall be provided in the manner and as per matrix and conditions specified in Schedule I.

"**Aadhaar Enabled Services**" shall mean services provided by an Authentication User Agency to Aadhaar Holder, using the Aadhaar Authentication Services of UIDAI.

"**Aadhaar Holder**" shall mean an individual who holds an Aadhaar Number.

"**Aadhaar Number**" shall mean the unique identification number issued to resident by UIDAI.

"**Agreement**" shall mean this agreement executed between the Parties, alongwith its schedules, annexures and exhibits, if any, and all instruments supplemental to or amending, modifying or confirming this agreement in accordance with the provisions of this agreement, if any, in each case as they may be supplemented or amended from time to time.

"**Authentication Device**" shall mean a terminal or device from where the Authentication User Agency carries out its service/business functions and interacts with Aadhaar Holders, by seeking authentication of Aadhaar Holders identity to enable the Authentication User Agency's business function.

"**Authentication Service Agency**" shall mean an entity providing compliant secured network connectivity to the UIDAI and the Authentication User Agency for enabling Aadhaar Authentication Services as separate agreements entered into between the entity and UIDAI and Authentication User Agency respectively.

"**Biometric Information**" shall mean ten finger prints and iris image, captured by UIDAI, as a part of the enrolment process for issuance of Aadhaar Number.

"**Business Day**" shall mean any day other than a Saturday, Sunday or official public holiday in India.

"**Central Identity Data Repository (CIDR)**" means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

"**Confidential Information**" shall mean any information which is considered confidential in terms of Clause 9 of this Agreement and shall include, but not limited to, information such as Aadhaar Number, name, address, age, date of birth, relationships and other demographic information, as also, biometric information such as finger print and iris scan of a resident.

"**e-KYC**" shall mean the transfer of demographic data (such as Name, Address, Date of Birth, Gender, Mobile number, Email address, etc.) and photograph collected by UIDAI in the form of a digitally signed XML document to an Authentication User Agency, through an Authentication Service Agency, based on resident authorization received by UIDAI in the form of successful biometric or OTP-based Aadhaar authentication.

"**False Accept**" shall be referred to a accept transaction where a system identifies a biometric as genuine (while, in reality it belongs some other individual) or will fail to reject an impostor biometric. Imposter can be defined as someone who intentionally or unintentionally is presenting his/her biometric against someone else's Aadhaar number.

"**KYC User Agency**" shall mean Authentication User Agency that is eligible for the e-KYC service.

"**KYC Service Agency**" shall mean Authentication Service Agency that is eligible to provide access to the e-KYC service through their network.

"**Law(s)**" shall mean all applicable laws, by-laws, rules, regulations, orders, ordinances, protocols, codes, guidelines, policies, notices, directions, judgments, decrees or other requirements or official directive of any governmental authority or person acting under the authority of any governmental authority, whether in effect or which may come into effect in the future.

"**OTP**" shall mean one time password sent to the Aadhaar holder's cell phone for the purpose of authentication.

358

"**Party**" refers individually to UIDAI and the Authentication User Agency and

"**Parties**" refer collectively to UIDAI and Authentication User Agency.

"**Personal Identity Data (PID)" refers to** Aadhaar-based Personal Identity Data/ Information including biometric and demographic information as well as the OTP used for Authentication

"**Standards**" shall mean the standards issued by UIDAI with regard to matters covered by this Agreement, and sole right of interpretation whereof shall rest with UIDAI at all times.

"**Sub-AUA**" shall mean an entity appointed by the Authentication User Agency under this agreement to access Aadhaar authentication services through the Authentication User Agency.

"**Term**" shall mean the duration specified in Clause 10.

"**Third Party**" shall mean any party who is not a Party.

1.2 Interpretation

1.2.1 In this Agreement, unless the context requires otherwise:

(i) reference to singular includes a reference to the plural and vice versa;

(ii) reference to any gender includes a reference to all other genders;

(iii) reference to an individual shall include his legal representative, successor, legal heir, executor and administrator;

(iv) reference to statutory provisions shall be construed as meaning and including references also to any amendment or re-enactment (whether before or after the date of this Agreement) for the time being in force and to all statutory instruments or orders made pursuant to statutory provisions;

(v) references to any statute or regulation made using a commonly used abbreviation, shall be construed as a reference to the title of the statute or regulation;

(vi) references to any Article, Clause, Section, Schedule or Annexure, if any, shall be deemed to be a reference to an Article, Clause, Section, Schedule or Annexure of or to this Agreement.

1.2.2 Clause headings in this Agreement are inserted for convenience only and shall not be used in its interpretation.

1.2.3 When any number of days is prescribed in this Agreement, the same shall be reckoned exclusively of the first and inclusively of the last day unless the last day does not fall on a Business Day, in which case the last day shall be the next succeeding day which is a Business Day.

1.2.4 If any provision in this Agreement is a substantive provision conferring rights or imposing obligations on anyone, effect shall be given to it as if it were a substantive provision in the body of this Agreement.

1.2.5 Any word or phrase defined in the body of this Agreement shall have the meaning assigned to it in such definition throughout this Agreement unless the contrary is expressly stated or the contrary clearly appears from the context.

1.2.6 The rule of construction, if any, that a contract shall be interpreted against the party responsible for the drafting and preparation thereof shall not apply.

1.2.7 Reference to days, months or years in this Agreement shall be a reference to calendar days, months or years, as the case may be, unless the contrary is expressly stated or clearly appears from the context.

1.2.8 Reference to any agreement, deed, document, instrument, rule, regulation, notification, statute or the like shall mean a reference to the same, as may have been duly amended, modified or replaced. For the avoidance of doubt, a document shall be construed as amended, modified or replaced only if such amendment, modification or replacement is executed in compliance with the provisions of such document(s).

2. APPOINTMENT OF AUTHENTICATION USER AGENCY

2.1 UIDAI hereby appoints the Authentication User Agency, as an Agency authorised to send requests for authenticating PID of Aadhaar Holder(s), subject to the terms and conditions of this Agreement.

2.2 The Authentication User Agency hereby unequivocally accepts its appointment as an Authentication User Agency, for providing Aadhaar Enabled Services to Aadhaar Holder(s), in terms of clause 2.1 above.

3. TERMS AND CONDITIONS OF APPOINTMENT OF AUTHENTICATION USER AGENCY

3.1 UIDAI hereby grants the Authentication User Agency a non-exclusive and revocable right to use Aadhaar Authentication Services, for providing Aadhaar Enabled Services to Aadhaar Holder(s), in the manner set out in this Agreement. The Authentication User Agency understands and agrees that it shall be responsible to UIDAI for all its Aadhaar authentication related aspects, covered by this Agreement, and in the event the Authentication User Agency outsources part(s) of its operations to other entities, the ultimate responsibility for the results of Aadhaar authentication related operations lies with the Authentication User Agency, and the Authentication User Agency shall ensure that the entity to which it has outsourced its operations is audited annually by information systems auditor certified by a recognized body. The Authentication User Agency also understands and agrees that it shall be responsible to UIDAI for all the Aadhaar authentication related aspects for all authentication requests which it transmits to the CIDR on behalf of Sub AUAs appointed by it. For avoidance of doubt, it is hereby expressly clarified that only entities contracted with UIDAI as an Authentication User Agency and their Sub AUAs shall be authorized to send request for authentication of PIDs of the Aadhaar holders. All the obligations of the Authentication User Agency under this agreement shall be equally applicable to the Sub AUAs. The Authentication User Agency understands that the Aadhaar Authentication Service shall be provided at the sole discretion of UIDAI, which reserves the right to add, revise, suspend in whole, or in part any of the Aadhaar Authentication Service, at any time with prior notice, in its sole discretion, for any reason whatsoever.

3.2 It is hereby mutually agreed between the Parties that the rights and obligations of the Authentication User Agency, under this Agreement, are non-transferable and non-assignable whether by sale, merger, or by operation of law, except with the express written consent of UIDAI.

3.3 The Authentication User Agency hereby unequivocally agrees that it shall use the Aadhaar Authentication Services, for providing Aadhaar Enabled Services to Aadhaar Holder(s), solely for the purposes set out in Schedule-II to this Agreement, and for no other purposes. In the event, the Authentication User Agency is desirous of using Aadhaar Authentication Services, for new and additional services/business functions without compromising or violating requirements specified by UIDAI with regard to network specifications, security etc., from time to time, it shall inform UIDAI in this regard

3.4 It is hereby expressly agreed between the parties that in cases where the Authentication User Agency or its Sub AUA forwards an authentication request to the Central Identity Data Repository, through an Authentication

Service Agency, and in the event of an Aadhaar authentication failure for whatever reasons, the Authentication User Agency may invoke other means of Identity authentication for service provision to the Aadhaar Holder, and the Authentication User Agency or its Sub AUA shall bear full responsibility for any decision taken in this regard and UIDAI shall have no role in this regard.

3.5 The Authentication User Agency hereby unequivocally agrees that all backend infrastructure, such as servers, databases etc., required specifically for the purpose of Aadhaar authentication shall be based in the territory of India.

3.6 The Authentication User Agency hereby unequivocally agrees that the use of the Aadhaar Authentication Services by it for providing Aadhaar Enabled Services to Aadhaar Holder(s) and the Aadhaar Authentication Services shall not, in any manner, whether direct or indirect, be used for purposes that are anti-government or anti-State or discriminatory or related to money laundering or in contravention of any laws applicable in India.

4. OBLIGATIONS OF UIDAI

4.1 UIDAI shall:

a) determine rules and frameworks regarding the usage of Aadhaar Number and Aadhaar Identity Data;

b) register/certify/approve, by itself or through approved independent certification agencies, all the applications & devices, such as applications driving the authentication systems in the Authentication User Agency's and Sub AUA's systems, that will be used by the Authentication User Agency;

c) determine and prescribe Standards and specifications for transmission of Aadhaar Identity Data for the purposes of Aadhaar Authentication Services and Aadhaar Enabled Services;

d) determine and prescribe Standards to ensure the confidentiality, privacy and security of Aadhaar Identity Data;

e) prescribe other Standards and specifications that UIDAI may deem necessary, in its sole judgment, for providing Aadhaar Authentication Services and Aadhaar Enabled Services;

4.2 Notwithstanding anything contained in Clauses 4.1 above, it is hereby clearly understood by the Parties that UIDAI shall have no responsibility or liability in relation to failures that may take place during the Aadhaar based authentication process, including but not limited to, failures as a result of, false reject, network or connectivity failure, device failure, possible down

time at Central Identities Data Repository, etc.

5. OBLIGATIONS OF THE AUTHENTICATION USER AGENCY

5.1 The Authentication User Agency shall, for every service/business function for which it is desirous of using Aadhaar Authentication Services, chooses suitable authentication type, for each particular service, from Aadhaar Authentication package Framework provided by UIDAI from time to time, which indicates the identity credentials (PID) to be sought from the Aadhaar Holder, who is seeking to access the specific service/business function(s). For avoidance of doubt, it is hereby expressly stated that the choice of authentication type(s), in the manner provided above, shall be the sole decision of the Authentication User Agency, and no other entity, including UIDAI, Authentication Service Agency and Aadhaar Holder shall have any role in this decision of Authentication User Agency.

5.2 The Authentication User Agency shall obtain a consent from the Aadhaar holder, for using the Aadhaar number and Biometric information for providing the Aadhaar Authentication Service

5.3 The Authentication User Agency hereby unequivocally agrees that it shall, forthwith, upon appointment as an Authentication User Agency, shall establish network connectivity, through an Authentication Service Agency, duly approved by UIDAI, with the Central Identities Data Repository, established by UIDAI that contains all Aadhaar Identity Data, in compliance with all the specifications and standards prescribed by UIDAI, from time to time. The Authentication User Agency assumes complete responsibility with regard to its network connectivity with an Authentication Service Agency. And UIDAI shall have no responsibility in this regard. Provided where the Authentication User Agency has entered into another agreement with the UIDAI to act as an Authentication Service Agency, such an Authentication User agency need not engage another Authentication Service Agency.

5.4 The Authentication User Agency shall establish and maintain necessary authentication related operations, including their own systems, processes, infrastructure, technology, security, etc., which may be necessary for providing Aadhaar Enabled Services, in compliance with standards and specifications, issued by UIDAI from time to time.

5.5 The Authentication User Agency shall ensure that the network connectivity between authentication devices and the Central Identities Data Repository, used for sending their authentication requests is in compliance with the standards and specifications issued by UIDAI from time to time. The

Authentication User Agency shall build and maintain the connectivity between authentication devices and the Authentication Service Agency's systems either by itself, or by outsourcing it to a service provider. The Authentication User Agency shall work with the Authentication Service Agency in ensuring the compliance of the connectivity between the Authentication Service Agency and Central Identities Data Repository.

5.6 The Authentication User Agency shall only employ the Authentication Devices and associated application components (such as sensor and extractor pairs for fingerprint and iris scanners) which are duly registered with/approved/certified by UIDAI or an agency appointed by UIDAI for this purpose. The Authentication User Agency understands the authentication type to be employed by it in providing Aadhaar Enabled Services and shall employ the Authentication Devices which confirm to the authentication type adopted by the Authentication User Agency, and UIDAI shall have no role to play in this regard, and shall have no liability or responsibility in this respect.

5.7 The Authentication User Agency shall install necessary Authentication Devices and other Information Technology devices along with device installation and maintenance kits, and the devices shall comply with specifications and standards prescribed by UIDAI from time to time. The Authentication User Agency shall ensure that the applications driving the authentication devices are duly registered with/approved/certified by UIDAI. The Authentication User Agency assumes complete responsibility for ensuring that the processes, procedures, systems and infrastructure at Authentication Device are in compliance with standards and specifications issued by UIDAI from time to time.

5.8 It is hereby expressly agreed between the Parties that in the event Authentication User Agency's federated authentication system includes Aadhaar authentication as well as the Authentication User Agency's local authentication system, the Authentication User Agency shall integrate their authentication systems with Aadhaar authentication system in compliance with standards and specifications issued by UIDAI from time to time.

5.9 The Authentication User Agency shall keep UIDAI informed of the Sub AUAs with whom they have entered into agreements and shall duly register them in the manner prescribed by UIDAI from time to time. The AUA shall issue a Sub AUA code to identify each Sub AUA and shall include the Sub AUA code in all authentication requests originating from that Sub AUA which it forwards to CIDR for authentication. The AUA shall keep the UIDAI informed of all Sub AUA codes that it issues. The Authentication User Agency shall ensure that the Sub AUAs comply with standards and protocols laid out by UIDAI from time to time. The Authentication User

364

Agency understands that it shall be responsible for all authentication requests originating from the Sub AUA and routed through the Authentication User Agency

5.10 The Authentication User Agency shall keep UIDAI informed of the list of Authentication Service Agency(ies) with whom they have any agreement(s), in the manner prescribed by UIDAI from time to time. The Authentication User Agency shall inform UIDAI, forthwith, all relevant information pertaining to any agreement that it may enter into with an Authentication Service Agency and any subsequent modifications thereto, if any. Authentication User agency is obligated to send the agreement entered with Authentication Service Agency immediately upon request from UIDAI. In the event the Authentication User Agency disengages with an Authentication Service Agency, the fact of disengagement shall be communicated to UIDAI, by the Authentication User Agency, within such period as may be prescribed by UIDAI from the date of disengagement.

5.11 The Authentication User Agency shall ensure that the persons employed by it for providing Aadhaar Enabled Services and for maintaining necessary systems, infrastructure, processes, etc. in this regard, possess requisite qualifications for undertaking such works. The Authentication User Agency shall be responsible for ensuring that, in case Authentication Devices are operated by its own or its agents personnel, such personnel are suitably and adequately trained to conduct Aadhaar Enabled Services, in compliance with specifications and standards prescribed by UIDAI from time to time.

5.12 The Authentication User Agency shall, at all times, comply with standards, directions, specifications, etc. issued by UIDAI, in terms of network and other Information Technology infrastructure, processes, procedures, etc. for the purposes of availing Authentication services provided by UIDAI. The Authentication User Agency shall be further responsible, at all times, for compliance with specification issued by UIDAI, from time to time, with respect to all authentication related aspects. In the event the Authentication User Agency outsources part(s) of its operations to other entities, the ultimate responsibility for the results of authentication related operations shall lie with the Authentication User Agency.

5.13 The Authentication User Agency shall, at all times, comply with the provisions contained in the Information Technology Act, 2000 and the statutory rules framed there under, from time to time, in so far the same has application to its operations in accordance with this Agreement, and also with all other Laws rules and regulations, whether already in force or which may be enacted anytime in the future, pertaining to data security

365

and management, data storage, sharing and data protection, as also with the National Identification Authority of India Bill, as and when the same is enacted into a law and comes into force, and shall ensure the same level of compliance by its Authentication Device.

5.14 The Authentication User Agency shall ensure that its operations and systems in terms of this Agreement are audited by information systems auditor certified by a recognized body on an annual basis to ensure compliance with UIDAI standards and specifications and the audit report should be shared with UIDAI upon request. In addition to the above, UIDAI may choose to, in its sole discretion, audit the AUA's operations and systems in terms of this Agreement by itself or through an auditor appointed by UIDAI, and the continuation of operations as the Authentication User Agency shall, at all times, be dependent upon the said audit confirming the compliance by the Authentication User Agency of the terms and conditions contained in this Agreement, and any failure in compliance of the same, if confirmed in the audit, may entail fine and/or penalties and termination of access to Aadhaar Authentication Services. "The Authentication User Agency unequivocally agrees to provide full co-operation to UIDAI or any agency approved and/or appointed by UIDAI in the audit process, and to provide to UIDAI or any agency approved and/or appointed by UIDAI, complete access to its procedures, records and information pertaining to services availed for UIDAI,

5.15 The Authentication User Agency shall monitor the operations of its Authentication Device, on a periodic basis, for compliance with the terms and conditions contained in this Agreement or with standards, directions, specifications, etc. issued and communicated by UIDAI, in this regard, from time to time.

5.16 The Authentication User Agency shall maintain logs of all authentication transactions processed by it, capturing the complete details of the authentication transaction, such as the Aadhaar number against which authentication is sought, authentication package, date and timestamp, etc. as prescribed by UIDAI from time to time but shall not, in any event, capture the PID information and shall retain the same for a duration, specified by UIDAI from time to time. The Authentication User Agency understands and agrees that the logs maintained by it shall be shared with any individual or entity only on a need-basis, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

5.17 In case of any investigations around authentication related fraud(s) or

dispute (s), the Authentication User Agency shall extend full cooperation to UIDAI, and/or any agency appointed/authorized by it and/or any other authorized investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resource/information, etc. of or pertaining to its Authentication Device.

5.18 The Authentication User Agency, where ever applicable, shall be responsible for identifying exception-handling mechanisms in the event of failure of Aadhaar Authentication Services.

5.19 The authentication charges, for providing Aadhaar Enabled Services by the Authentication User Agency to its customers, shall be evolved by the Authentication User Agency and UIDAI shall have no say in this respect, for the time being, however, UIDAI's right to prescribe a different mechanism in this respect, in the future, shall be deemed to have been reserved.

5.20 The Authentication User Agency unequivocally agrees that all devices and applications used by it in running its Aadhaar authentication operations shall be duly certified/approved by UIDAI or an agency appointed/ approved by UIDAI (as and when UIDAI creates a certification mechanism for certifying Aadhaar enabled application). In the event the already certified/approved applications employed by the Authentication User Agency undergo modifications, the Authentication User Agency shall deploy the modified applications only after renewed certification/approval from UIDAI.

5.21 The Authentication User Agency agrees to incorporate and adopt standards, specifications and other terms and conditions as prescribed by UIDAI from time to time, in its agreement with the ASA for the purpose of availing Authentication services of UIDAI.

5.22 Authentication User Agency hereby agrees to inform UIDAI of any misuse of Aadhaar data or any compromise of Aadhaar related data or systems within their network.

6. REPRESENTATIONS AND WARRANTIES

6.1 UIDAI represents and warrants to the User Authentication Agency that:

(a) UIDAI is an authority set up by the Planning Commission, Government of India;

(b) UIDAI has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;

(c) this Agreement has been validly executed by UIDAI and constitutes a valid agreement binding on UIDAI and enforceable in accordance with the laws of India;

6.2 The Authentication User Agency represents and warrants to UIDAI that:

(a) the User Authentication Agency is an entity legally constituted and validly existing under the laws of India;

(b) the User Authentication Agency has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;

(c) this Agreement has been validly executed by the User Authentication Agency and constitutes a valid agreement binding on the Authentication User Agency and enforceable in accordance with the laws of India.

7. INTELLECTUAL PROPERTY

7.1 The Authentication User Agency is aware that "Aadhaar" is the intellectual property of UIDAI and the Authentication User Agency understands that any unauthorized reproduction of the same constitutes infringement and may be subject to penalties, both civil and criminal.

7.2 It is hereby mutually agreed between the Parties that the Authentication User Agency shall have a non-exclusive right to use the Aadhaar name and logo and to represent itself as an entity providing Aadhaar Enabled Services to Aadhaar Holder(s), subject to the condition that all rights, title and interest, including intellectual property rights, in the Aadhaar name and logo shall vest, at all times, either during the operation of this Agreement or otherwise, in UIDAI.

7.3 The Authentication User Agency hereby unequivocally agrees that it shall use the Aadhaar name and logo, without any modification, in its promotional, educational and informational literature, for the duration of this Agreement.

7.4 The Authentication User Agency hereby unequivocally agrees that it shall not authorize any other entity or individual to use the Aadhaar name and logo, except with the prior written permission of UIDAI.

7.5 The Authentication User Agency hereby unequivocally agrees that upon becoming aware of unauthorized use, copy, infringement or misuse of the

Aadhaar name and/or logo, and any rights, title and interest therein, including intellectual property rights, it shall notify UIDAI about such unauthorized use forthwith. At the request and cost of UIDAI, the Authentication User Agency shall take part in or give assistance in respect of any legal proceedings and execute any documents and do any things reasonably necessary to protect the rights, title and interest of UIDAI, including intellectual property rights, in respect of the Aadhaar name and logo.

8. INDEMNITY AND LIMITATION OF LIABILITY

8.1 The Authentication User Agency understands that the use of Aadhaar Authentication Services by the Authentication User Agency does not result in incurring of any liability by UIDAI whatsoever. The Authentication User Agency alone is responsible for the proper and judicious use of the Aadhaar Authentication Services. UIDAI shall not, in any case, be held responsible for damage and/or harm, direct or indirect, material or immaterial, or of any nature whatsoever, arising from any unavailability of the Aadhaar Authentication Services or its use by the Authentication User Agency except the damages which solely arising out of false acceptance by UIDAI biometric authentication services..

8.2 It is hereby mutually agreed between the Parties that UIDAI shall not be liable for any unauthorized transactions occurring through the use of Aadhaar Authentication Services and the Authentication User Agency hereby fully indemnifies and holds UIDAI harmless against any action, suit, proceeding initiated against it or any loss, cost or damage incurred by it as a result thereof.

8.3 Without prejudice to generality of the above, the Authentication User Agency shall indemnify and keep UIDAI harmless and indemnified from and against all claims, liabilities, losses and incurred costs, fines, penalties, expenses, taxes, assessment, punitive damages, fees (including advocate's/ attorney's fee), liabilities (including any investigative, legal and other expenses incurred in connection with, and any amounts paid in settlement of, any pending or threatened legal action or proceeding), judgments, awards, assessments, obligations, damages, etc., which UIDAI may suffer or incur arising out of, or in connection with:

a) any act, neglect, default or omission on the part of the Authentication User Agency, its subsidiaries or any person associated with the Authentication User Agency, including but not limited to liabilities arising from non compliance of Standards and Regulations prescribed by UIDAI, from time to time, unauthorized use or disclosure of Confidential Information and failure to comply with data protection and storage requirements, as prescribed by UIDAI, from time to time;
b) any breach by the Authentication User Agency of the terms and conditions or its appointment or its obligations under this Agreement;
c) any breach by the Authentication User Agency of its obligations under any Law(s) or contract, etc;
d) default or omission on the part of the Authentication User Agency to

follow statutory instructions and guidelines issued by the Government of India, National Identification Authority of India (as and when setup) and any other governmental authority.

8.4 In the event of a Third Party bringing a claim or action against UIDAI, as a consequence of the use of Aadhaar Authentication Services by the Authentication User Agency or its Sub AUA, the Authentication User Agency shall:

a) defend and / or to assist UIDAI in defending, at the Authentication User Agency's cost, such claims or actions, either in a legal proceeding or otherwise;

b) indemnify UIDAI and keep UIDAI indemnified and harmless, at all times, against all actions, claims, demands, costs, charges and expenses arising out of or incurred by reason of any infringement of intellectual property rights of any Third Party in connection with the use of the Aadhaar Authentication Services, irrespective of whether or not UIDAI incurs any liability in this regard by virtue of any judgment of a court of competent jurisdiction.

8.5 The Authentication User Agency is aware of, and understands, the fact that UIDAI's operation of the Aadhaar Authentication Services is not completely free from defect, and UIDAI does not represent and warrant the same to be defect free. Unless otherwise expressly specified in writing, the Aadhaar Authentication Services are provided on an 'as is' basis, without any express or implied warranties in respect thereof. It is hereby mutually agreed between the Parties that under no circumstances shall UIDAI be

liable for any damages whatsoever, whether such damages are direct, indirect, incidental consequential and irrespective of whether any claim is based on loss of revenue, interruption of business or any loss of any character or nature whatsoever and whether sustained by the Authentication User Agency or by any other person, as a result of the operation of this Agreement or otherwise except the damages which solely arising out of false acceptance by UIDAI biometric authentication services..

8.6 The maximum liability for which UIDAI may be held responsible in respect of a false acceptance shall be restricted to the amount of that transaction or the actual unrecovered direct loss to the Authentication User Agency or maximum amount of liability fixed by UIDAI time to time , whichever is less Provided that:

a) The Authentication User Agency actually suffers a direct loss of the said amount, and there being no recourse of recovery thereof from the incorrect beneficiary account or

b) Where recourse does exist, it would be incumbent on the Authentication User Agency to diligently pursue recovery and where recovery either partial or full, has been effected, the liability of UIDAI would stand reduced by that extent.

The liability as mentioned above will be subject to the Compliance by Authentication User Agency of all the procedures, standards and specification as prescribed by UIDAI from time to time in this regard.

8.7 It is hereby mutually agreed that this Clause 8 shall survive the termination of this Agreement.

9. CONFIDENTIALITY, DATA PROTECTION, SECURITY AND USE OF INFORMATION

9.1 The Authentication User Agency and all its Sub AUAs shall treat all information, which is disclosed to it as a result of the operation of this Agreement, as Confidential Information, and shall keep the same confidential, maintain secrecy of all such information of confidential nature and shall not, at any time, divulge such or any part thereof to any third party except as may be compelled by any court or agency of competent jurisdiction, or as otherwise required by law, and shall also ensure that same is not disclosed to any person voluntarily, accidentally or by mistake.

9.2 The Authentication User Agency shall use the Confidential Information strictly for the purposes of authentication of the Aadhaar Holder, and for providing Aadhaar Enabled Services, in accordance with this Agreement. The Authentication User Agency shall ensure compliance with all

371

applicable laws and regulations including but not limited to regulations on data protection under the Information Technology Act, 2008 when collecting information from residents for their business purposes.

9.3 The Authentication User Agency shall scrutinize the data collected by it, while processing authentication requests, on a periodic basis, and shall preserve such data collected in relation to an authentication request until such as may be prescribed by UIDAI from time to time.

9.4 The Authentication User Agency is prohibited from storing any PID in their data base or in any storage device of any nature whatsoever including Authentication Device or in any machine, device or instrument of any kind whatsoever, removable storage devices or in physical form, at point in time.

9.5 The Authentication User Agency hereby unequivocally agrees to undertake all measures, including security safeguards, to ensure that the information in the possession or control of the Authentication User Agency, as a result of operation of this Agreement, is secured and protected against any loss or unauthorised access or use or unauthorised disclosure thereof.

9.6 It is hereby mutually agreed between the parties that UIDAI assumes no responsibility or liability for any action or inaction, use or misuse of the Confidential Information and other data in the control of the Authentication User Agency. The Authentication User Agency agrees and acknowledges that any loss, damage, liability caused or suffered by the Authentication User Agency due to disclosure of all information of confidential nature shall be borne by Authentication User Agency without transferring any liability or responsibility towards UIDAI.

9.7 It is hereby mutually agreed that this Clause 9 shall survive the termination of this Agreement.

10. TERM, TERMINATION AND CONSEQUENCES

10.1 This Agreement shall be in force for a period of _____ years from the Effective Date, unless renewed by mutual consent, in writing, of the Parties, prior to expiry of this Agreement, upon such terms and conditions as may be mutually agreed between the Parties.

10.2 UIDAI shall have the right to terminate this Agreement by giving thirty (30) days notice, in writing, prior to expiry of the Term, without any protest or demur from the Authentication User Agency, in the event of the Authentication User Agency:

a) fails to comply with the Standards or the decision and directions issued by UIDAI, from time to time, with regard to the interpretation and enforcement of the Standards;

b) is in breach of its obligations under this Agreement;

c) uses the Aadhaar Authentication Services for any other purpose than those specified in Schedule-II of this Agreement;

d) is in liquidation, or if a receiver has been appointed in respect of the Authentication User Agency or the Authentication User Agency becomes subject to any form of insolvency administration or files for voluntary liquidation.

e) In case the AUA is also an ASA, termination of the ASA agreement with UIDAI will automatically terminate this agreement.

10.3 The Authentication User Agency shall have no right to compensation for termination of this Agreement by UIDAI, in pursuance of clauses 10.2 above.

10.4 The termination of this Agreement by UIDAI, in pursuance of clauses 10.2 above, shall result in automatic cancellation of the registration of the Authentication User Agency, granted by UIDAI, without any notification, in this regard, to the Authentication User Agency.

10.5 The Authentication User Agency may terminate this agreement by giving 30 days' notice in writing to the UIDAI.

10.6 Upon termination of this Agreement, the Authentication User Agency shall, forthwith, cease to use the Aadhaar name and logo for any purposes, and in any form, whatsoever.

11. FORCE MAJEURE

11.1 The Parties agree that neither of them shall be liable to the other for any loss, delay, damage or other casualty suffered or incurred by the other owing to earthquakes, floods, fires, explosions, acts of God, acts of State, war, terrorism, action of any governmental authority or any other cause, which is beyond the reasonable control of that Party ("**Force Majeure**") and any failure or delay by any Party in the performance of any of its obligations under this Agreement owing to one or more of the foregoing causes shall not be considered as a breach of any of its obligations under

this Agreement. The Parties however agree that any financial failure or non-performance of any financial obligations or covenants of the Parties shall not constitute Force Majeure.

11.2 The Party claiming benefit of Force Majeure shall however not be entitled to the same unless it has intimated the other Party of the occurrence of such event within a period of seventy two (72) hours from the occurrence of such Force Majeure event indicating therein the steps that it is taking or intending to take to mitigate the effect of such Force Majeure on the performance of his obligations under this Agreement.

11.3 In the event, the Force Majeure event continues for a period of more than ninety (90) days, the Party shall renegotiate this Agreement in good faith and if the Parties do not reach any consensus on modifications to this Agreement within a period of one hundred twenty (120) days from the date of occurrence of the Force Majeure event, this Agreement shall automatically stand terminated on such date.

12. GOVERNING LAW AND DISPUTE RESOLUTION

12.1 This Agreement shall, in all respects, be governed by, and construed in accordance with the laws of India.

12.2 Any dispute of whatever nature, which arises out of, in relation to, or otherwise connected with:

(a) the interpretation or effect of;

(b) the validity, enforceability or rectification (whether in whole or in part) of;

(c) the respective rights or obligations of the Parties; and/or

(d) a breach (including a breach of any representation and warranty and/or the materiality thereof and/or the amount of compensation payable in order to remedy such breach and/or the breach or failure to comply with any covenants or undertakings contained herein) or the termination or cancellation of, this Agreement or in regard to whether either Party have unreasonably withheld its approval or consent under circumstances in which it may not do so; shall be dealt with in accordance with succeeding provisions of this Clause 12.

(All disputes arising out of reasons mentioned herein-above shall be collectively referred to hereinafter as a "**Dispute(s)**").

374

12.3 All Disputes shall at the first instance be resolved through good faith negotiations, which negotiations shall begin promptly after a Party has delivered to the other Party a written request for such consultation.

12.4 If the Parties are unable to resolve the Dispute in question within thirty (30) days of the commencement of negotiations in terms of Clause 12.3, then the Dispute shall, unless the Parties otherwise agree in writing, be referred for determination in accordance with the remaining provisions of this Clause 12.

12.5 The Dispute shall be referred to arbitration in accordance with the provisions of the (Indian) Arbitration and Conciliation Act, 1996.

12.6 The venue for arbitration shall be New Delhi, India and the language used in the arbitral proceedings shall be English.

12.7 The reference shall be referred to arbitration of an Arbitrator, to be nominated by Secretary, Department of Legal Affairs ("Law Secretary"). The award of the Arbitrator shall be binding upon Parties to the dispute.

12.8 The decision of the Arbitrator appointed to deal with such matters shall be accepted by the Parties as final and binding.

12.9 The Parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration.

12.10 The Parties shall use their best endeavors to procure that the decision of the Arbitrators shall be given within a period of six (6) months or soon thereafter as is possible after it has been demanded.

12.11 This Clause 12 is severable from the rest of this Agreement and shall remain in effect even if this Agreement is terminated for any reason.

12.12 The Courts in New Delhi, India shall have exclusive jurisdiction in relation to this Agreement, including this Clause 12.

12.13 All fees and costs pertaining to arbitration proceedings shall be borne equally by the Parties.

12.14 All other fees and costs incurred by the Parties shall be borne by the respective Parties.

13. GENERAL

13.1 Notices

Any notice, direction or other documentation required or remitted to be given hereunder shall be in writing and may only be given by personal delivery, international courier, electronic mail or facsimile (with confirmation received) at the addresses hereinafter set forth:

(i) For UIDAI :

Address	:	3rd Floor, Tower II, Jeevan Bharati Building Connaught Circus New Delhi-110001
Attention	:	Asstt. Director General - Authentication
Fax No.	:	011 - 23752679

(ii) For the Authentication User Agency :

Address	:	_____ _____ _____
Attention	:	_____
Fax No.	:	_____

13.2 Further Assurances

The Parties hereto shall sign such further and other papers, cause such meetings to be held, resolutions passed and bylaws enacted, exercise their vote and influence, do and perform and cause to be done and performed such further and other acts and things as may be necessary or desirable in order to give full effect to this Agreement and every part hereof.

13.3 No Waiver

No failure by a Party to take any action with respect to a breach of this Agreement or a default by any other Party shall constitute a waiver of the former Party's right to enforce any provision of this Agreement or to take action with respect to such breach or default or any subsequent breach or default. Waiver by any Party of any breach or failure to comply with any provision of this Agreement by a Party shall not be construed as, or constitute, a continuing waiver of such provision, or a waiver of any other

breach of or failure to comply with any other provision of this Agreement, unless any such waiver has been consented to by the other Party in writing.

13.4 Severability

If any Clause or part thereof, of this Agreement or any agreement or document appended hereto or made a part hereof is rendered invalid, ruled illegal by any court of competent jurisdiction, or unenforceable under present or future Laws effective during the term of this Agreement, then it is the intention of the Parties that the remainder of the Agreement, or any agreement or document appended hereto or made a part hereof, shall not be affected thereby unless the deletion of such provision shall cause this Agreement to become materially adverse to any Party in which case the Parties shall negotiate in good faith such changes to the Agreement, or enter into suitable amendatory or supplementary agreements, as will best preserve for the Parties the benefits and obligations under such provision.

13.5 Enurement

Upon receipt of consent from UIDAI as required in Clause 3.2 this Agreement will enure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns.

13.6 Counterparts

This Agreement may be executed in one or more counterparts, all of which shall be read and construed as one document and any facsimile signature hereto shall be deemed to be an original signature.

13.7 Independent Legal Advice

Each of the Parties acknowledges that it has received independent legal advice regarding the terms of this Agreement.

13.8 Entire Agreement

This Agreement constitutes the entire agreement between the Parties. There are not and will not be any verbal statements, agreements, assurances, representations and warranties or undertakings among the Parties and this Agreement may not be amended or modified in any respect except by written instrument signed by the Parties.

13.9 Independence of the Parties with respect of each other

Each of the Parties is and shall remain independent parties. Neither Party nor any of their respective affiliates shall have the authority to enter into

any contract or any obligation for, or make any warranty or representation on behalf of the other.

13.10 Expenses

Each of the Parties shall bear the fees and expenses of their respective counsels, accountants and experts and all other costs and expenses as may be incurred by them incidental to the negotiation, preparation, execution and delivery of this Agreement.

13.11 Surviving Provisions

13.11.1 The provisions of this Agreement, which are intended to survive the term of this Agreement by their very nature, shall survive the termination of this Agreement.

13.11.2 Notwithstanding the generality of the above, Clauses 8, 9 and 12 shall survive the termination/expiration of this Agreement.

13.12 Assignment

This Agreement shall not be assigned by either Party without obtaining a prior written consent from the other.

IN WITNESS WHEREOF the parties have each executed this Agreement by its duly authorized officer as of the day and year first above written.

SIGNED AND DELIVERED FOR AND ON BEHALF OF **THE UNIQUE IDENTIFICATION AUTHORITY OF INDIA**

Title: _____

Designation: _____

Signature: _____

SIGNED AND DELIVERED FOR AND ON BEHALF OF

_____

Title: _____

Designation: _____

Signature: _____

WITNESSES:

Title: _____ Title: _____

Signature: _____ Signature: _____

379

SCHEDULE I
(Aadhaar Authentication Services – operation metrics and conditions)

1. The system designed by UIDAI for providing authentication services shall be available across multiple data centres. Other than planned outage the system is expected to run at 99.7% uptime.

2. The CIDR response time is expected to be between 1 to 3 seconds.

3. In order to ensure that the authentication service is friendly to the resident Aadhaar holder it is important that the authentication user agency and sub authentication user agency provide an efficient application to maintain end use latency under 5 seconds. AUAs/Sub-AUAs should consider round trip network latency from their devices to UIDAI data center and back while planning service roll out on the field. Depending on the choice of network and bandwidth, on the field performance may vary. It is important that for a good resident experience, AUAs/Sub-AUAs should try to keep the full round trip service time to be less than 8-10 seconds on an average.

4. In situations where OTP is being used as a factor for authentication, the delivery of the OTP to the Aadhaar number holder depends on SMS/Email delivery which is not in the control of UIDAI as these services are provided by external service providers. It is expected that OTP will be delivered within a reasonable time. AUAs/Sub-AUAs are encouraged to use OTP API to ensure reliability of inbound OTP request. OTP validity is specified within the message to make it easier and is currently kept at 30 min.

380

SCHEDULE- II

Purposes for which Aadhaar Authentication Services shall be used by the Authentication User Agency

381

ANNEXURE 1

e-KYC Agreement
(Annexure to UIDAI - AUA agreement)

1. Terms and Conditions

i. Aadhaar e-KYC is an Aadhaar Enabled Service offered by the UIDAI through the Authentication Service Agencies to Authentication User Agencies.

ii. Aadhaar e-KYC service is offered free of charge till a pricing policy decision is announced by UIDAI.

iii. UIDAI hereby grants the Authentication User Agency a non-exclusive and revocable right to use the Aadhaar e-KYC service to provide services to Aadhaar Holders. The Authentication User Agency understands that the Aadhaar e-KYC Service shall be provided at the sole discretion of UIDAI, which reserves the right to add, revise, suspend in whole, or in part any of the Aadhaar e-KYC Service, at any time with prior notice, in its sole discretion, for any reason whatsoever. All the obligations of the Authentication User Agency under this agreement shall be equally applicable to the sub-AUAs.

iv. The Authentication User Agency hereby unequivocally agrees that all backend infrastructure, such as servers, databases etc., required specifically for the purpose of Aadhaar e-KYC shall be based in the territory of India.

v. It is hereby clearly understood by the Parties that UIDAI shall have no responsibility or liability in relation to failures that may take place during the Aadhaar e-KYC process.

2. Obligations of UIDAI

UIDAI shall:

i. Provide e-KYC data to the Authentication User Agency through the Authentication Service Agency upon authorization of the e-KYC request by an Aadhaar Holder, in the form of successful biometric or OTP-based Aadhaar authentication;

ii. Provide the e-KYC data in a manner conformant to the standards and processes described in the Demographic Data Standards and Verification Procedure (DDSVP) Committee Report;

382

iii. Provide e-KYC data conforming to Section 3 (Authentication of electronic Records), Section 4 (Legal recognition of electronic records), Section 5 (Legal recognition of digital signatures) and Section 6 (Use of electronic records and digital signatures in Government and its agencies) of the Information Technology Act, 2000;

iv. Determine and prescribe Standards and specifications for transmission of Aadhaar Identity Data for the purposes of Aadhaar e-KYC services,

v. Determine and prescribe standards to ensure the confidentiality, privacy and security of e-KYC data;

3. Obligations of Authentication User Agency

i. The Authentication User Agency shall maintain logs of all e-KYC transactions processed by it, capturing the complete details of the e-KYC transaction, such as the Aadhaar number against which e-KYC is sought, transaction code, authentication type, requesting AUA, requesting authentication device, date and timestamp, etc. as prescribed by UIDAI from time to time. The Authentication User Agency understands and agrees that the logs maintained by it shall be shared with any individual or entity only on a need-basis, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

ii. The e-KYC data resulting from an e-KYC request contains PII data for the purposes of service delivery. The storage of e-KYC data shall comply at all times with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

iii. The e-KYC data shall not be used by the AUA for purposes other than that for which the resident has explicitly given his/her consent.

iv. The AUA shall not share the e-KYC data with any other agency for whatsoever purposes.

v. The AUA shall be responsible for obtaining the authentication consent (biometric or OTP based) of the resident for authentication by UIDAI to transfer his/her e-KYC details to the designated service provider.

vi. The AUA shall maintain records of obtaining the consent of the resident for a time period specified by UIDAI and allow access to UIDAI or any entity authorized by it to the related records.

DIFFERENCE BETWEEN BORDER CONTROL SYSTEM AND AADHAAR SYSTEM

Sr.	Particulars	Aadhaar System	Border Control System
1.	Purpose	Provide universal identity and facilitate administration	Maintain record of entry of foreigners for national security
2.	Information collected	Biometric and demographic data **(Page 32 ofcompilation Vol I)**	Biometric and demographic data
3.	Place of collection of biometrics	Enrolment centre set up by private enrolment agencies egoffices of private entities, public or private sector banks etc **(Page 31 ofcompilation Vol I)**	Airports
4.	Persons giving the information	Each and every individual (citizen and resident)	Only foreign residents entering the country
5.	Party collecting the finger prints	Private entities **(Page 29 ofcompilation Vol I)**	Airport authorities
6.	Centralisation of database	Centralisation of every individual's information in a single database **(Page 33 ofcompilation Vol I)**	Local databank for limited purpose
7.	Data sharing	Centralised data shared with state and private sector entities **(page 38 of compilation Vol I)**	No data policy
8.	Authentication	Authentication for each and every service by Government and private agencies **(page 141 of compilation Vol II)**	No authentication for services
9.	Real time verification	Real time verification within 1-10 seconds **(page 143 of compilation Vol II)**	No verification as no requirement to authenticate for availing services

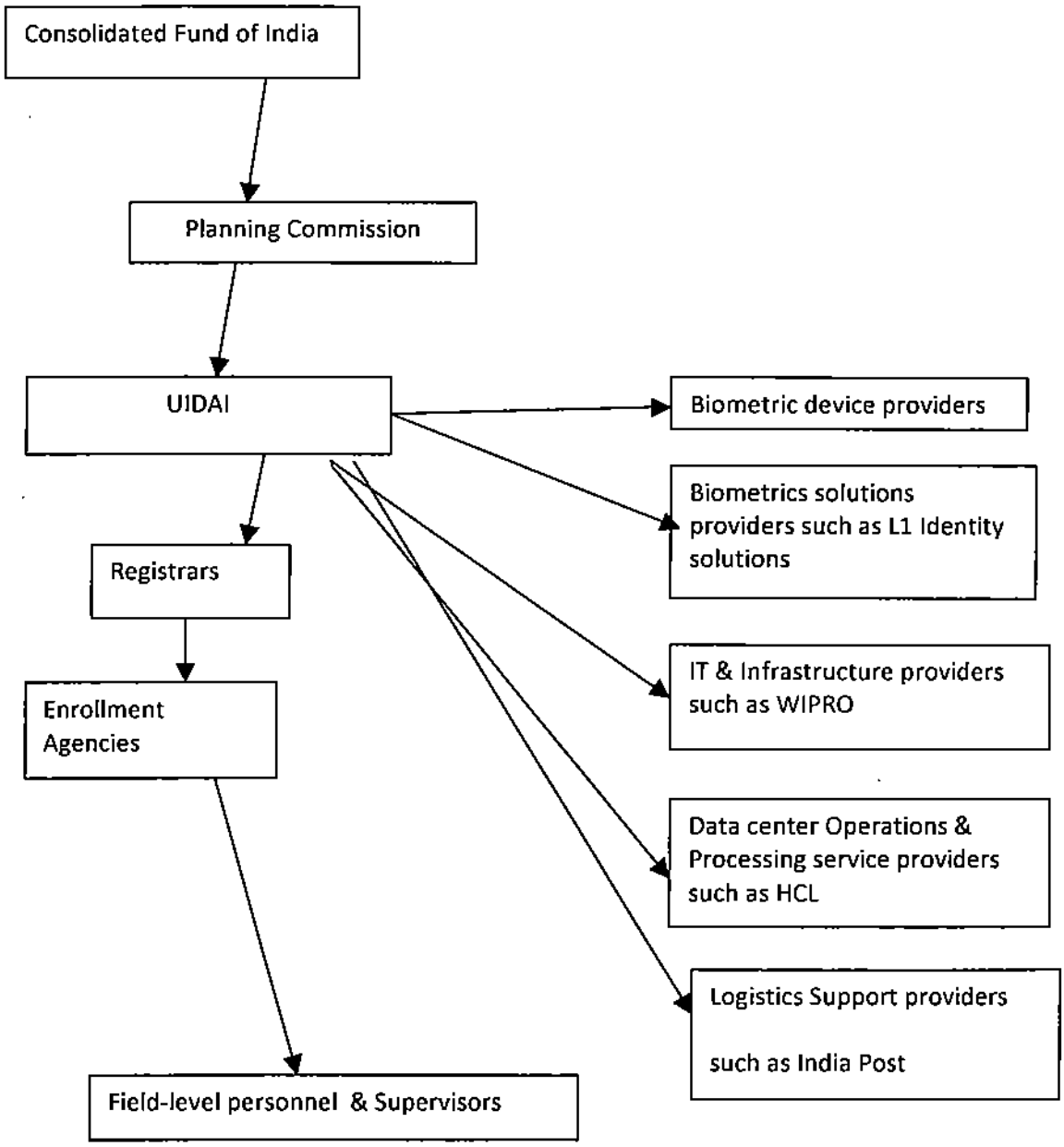
Information collected by EAs

Biometric Information	Non-biometric demographic information	Other Info
Fingerprints (10 fingers) Iris scan (2 eyes) Facial Photograph	**Primary information** Name Gender Date of Birth Residential Address **Additional Information** Mobile No Email **Financial Information** Bank A/C No. **Know-Your-Resident-Plus fields (For Registrar)** Panchayat name EPIC No. MNREGA Job card no. Pension Type Post office Account number Ration card details	**Introducer's** Aadhaar no. **Consent** for UIDAI to share information with other agencies. **Id proofs** such as PAN no. Driving licence or other photo identity cards. (List of 18 documents) **Address proofs** such as telephone bill, bank passbook, ration card, water bill, electricity bill etc. (List of 33 documents) **Proof of relationship document** like the head of the family's PDS Card, MNREGA card etc (list of 8 documents) **Proofs of DOB** (SSLC certificate etc. List of 4 documents)

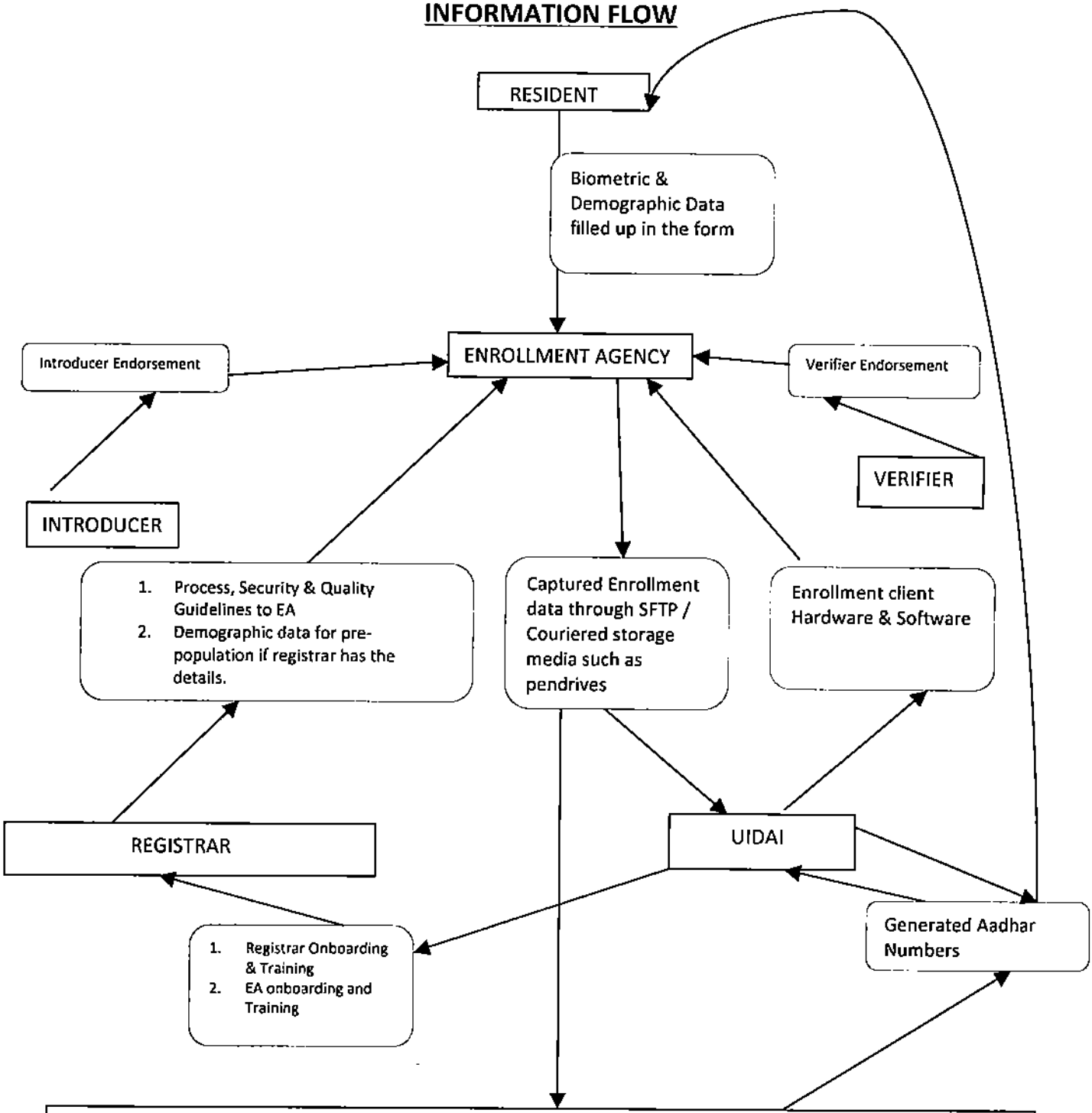
DISTINCTION BETWEEN THE AADHAAR AND COLLECTION OF FINGER PRINTS UNDER SECTION 32A OF THE REGISTRATION ACT, 1908.

No.	Particulars	Aadhaar	Registration Act, 1908
1.	Purpose	Facilitate administration	Record and verification of title
2.	Nature of biometric information	All ten finger prints and iris	Finger prints
3.	Nature of demographic information	Name, Address, Telephone, Bank details, credit card details, etc	No information to government. The information mentioned in the document is only for the parties.
4.	Legal Requirement	No legal sanction for collecting biometric information	Legislative backing in form of Section 32A
5.	Knowledge of intended purpose	No information to the individual of pitfalls of this project such as commercial use, surveillance, tracking, arbitrary police action	Only to ensure authenticity of document
6.	Place of collection of finger prints	Shops/offices of private entities, public sector banks or private sector banks etc	Office of Sub-Registrar
7.	Party giving the finger prints	Each and every individual (Citizen and resident)	Only persons seeking registration of documents requiring registration under law
8.	Party taking the finger prints	Private entities	Sub-Registrar's and other designated officers
9.	Platform on which the finger prints are captured	Computers/laptops/scanners and other devices	Original **Paper Document** executed by parties
10.	Portability of data	Pend Drives/Hard disks/file transfer protocols for submitting the data to UIDAI	No transfer of data
11.	Centralisation of database	Centralisation of each and every enrolment in a single database	No centralisation
12.	Scope of retention and duplication	Involves substantial risks of duplication	Cannot be duplicated in any manner
13.	Scope of misuse	Can be misused for commercial purpose, arbitrary police action etc	No scope for misuse
14.	Authentication	Authentication for each and every service by Government and non-government agencies	No scope for authentication
15.	Allocation of identity number with finger prints	Each biometric is allotted a corresponding number i.e Aadhaar number	No allocation of number identifying the biometric

FUNDS FLOW


Consolidated Fund of India
Planning Commission
UIDAI
Registrars
Enrollment Agencies
Field-level personnel & Supervisors
Biometric device providers
Biometrics solutions providers such as L1 Identity solutions
IT & Infrastructure providers such as WIPRO
Data center Operations & Processing service providers such as HCL
Logistics Support providers such as India Post

INFORMATION FLOW



1. Centers in Manesar & Bangalore.
2. Data center and Data processing operated by HCL Infosystems etc.
3. IT Infrastructure provided by Wipro etc.
4. Deduplication & Authentication solutions provided by companies such as L1 Identity Solutions etc.
5. Data received, Deduplication (Automatic Biometric & Manual Demographic deduplication) performed and Aadhaar generated.

389

A Delhi Lawyer living in Noida, appearing in Delhi on Tuesday, and Bombay on Wednesday.

6 AM

9 AM

9.30 AM

TOLL PLAZA

COURT

10.15 AM

1 PM

4.30 PM

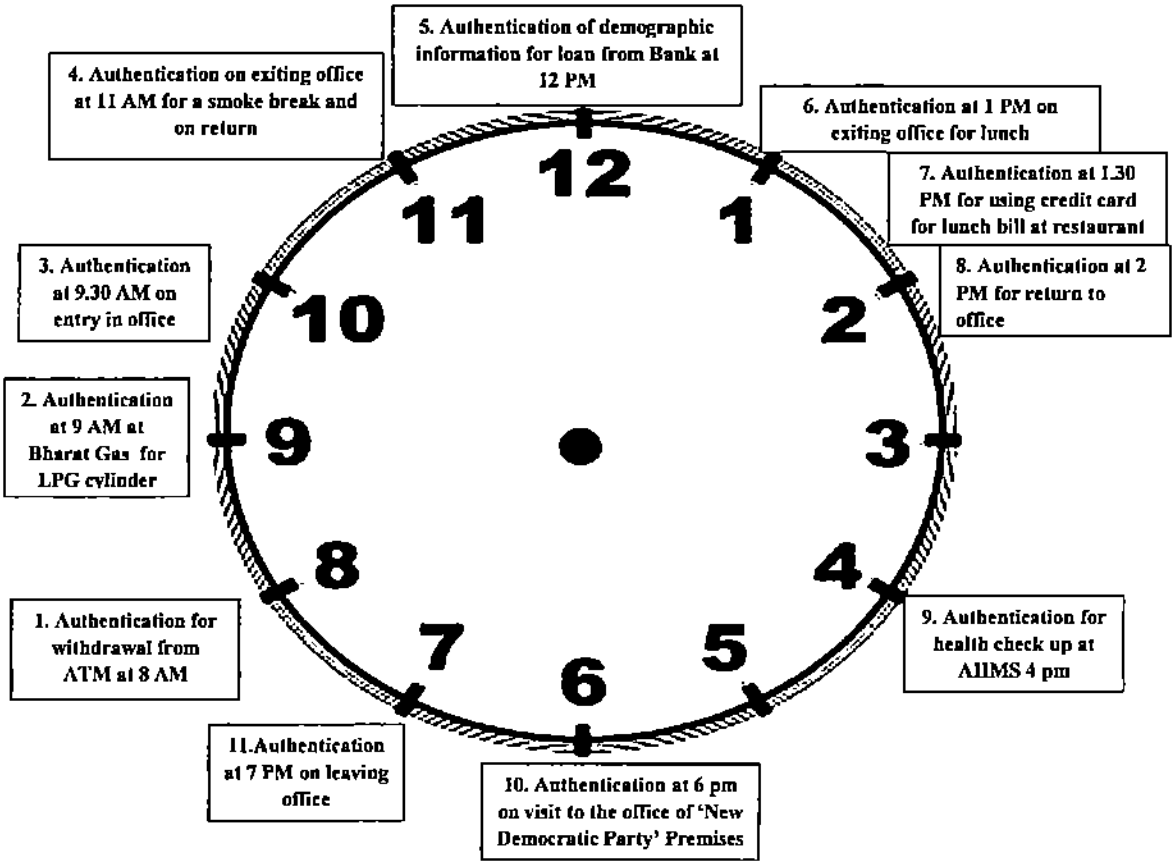
5 PM

AIRPORT

8.45 PM

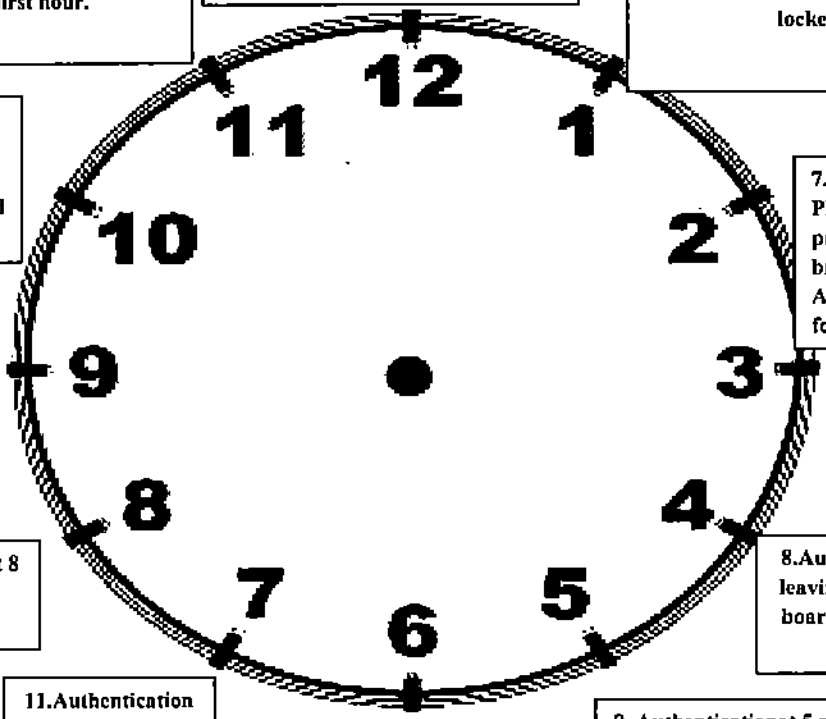
11 PM

REAL TIME INFORMATION OF MR. PAREKH IN UIDAI's AADHAAR AUTHENTICATION SYSTEM



- Points 1 and 7 above are covered under RBI circular dated 26.11.2013 which requires biometric authentication for using debit/credit cards. (Annexure -3 to Additional Affidavit filed by Petitioners in WP 829 of 2013)
- Point 2 is covered by Direct Benefit Transfer (DBT) for LPG cylinders introduced by Ministry of Petroleum.
- Point 3, 4, 6, 8, 10 & 11 is already used by offices and law firms for entry and exit of its employees
- Point 5 is covered under services contemplated under 'UIDAI Strategy Overview' (page 95 of UIDAI Counter Affidavit Vol II)
- Point 9 is covered under services contemplated under 'UIDAI Strategy Overview'

IN THE WAKE OF AADHAAR - A DAY IN THE LIFE OF A TEACHER Ms. SITA PARWAR.



1. Authentication at 8 AM to recharge mobile phone.

2. Authenticationat 9 AM while boarding on school bus. (She has to prove she is she after all. Principal needs

3. Aadhaar-enabled Attendance at school for her and her pupils

4. More authentication at the end of the first hour.

5. Authentication to exit school and enter bank and drop a draft at 12 noon.

6. Authenticationat 1PMto access the Aadhaar-enabled lunch box locker.

7. Authenticationat 2 PM for entering principal's office for a brief meeting. Authentication again for entering class.

8.Authenticationfor leaving school. And boarding the school bus.

9. Authenticationat 5 pm on visit to nearby ATM to withdraw money.

10.Authentication at 6 PM at police station while visiting to report the loss of the room-mate's mobile phone.

11.Authentication at 7 PM at the nearby supermarket while buying vegetables for dinner.

UID – the convergence point.

393

	uid	first_name	last_name
1	123456789011	Veeru	Sharma
2	123456789012	Jai	Dev
3	123456789013	Rahim	Ahmed
4	123456789014	Basanti	Dutta
5	123456789015	Gabbar	Singh
6	123456789016	Radha	Radha

UID Database

	uid	first_name	last_name	account_balance
1	123456789013	Rahim	Ahmed	435970.27
2	123456789012	Jai	Dev	435969.34
3	123456789014	Basanti	Dutta	435971.21
4	123456789016	Radha	Radha	435973.07
5	123456789011	Veeru	Sharma	435968.41
6	123456789015	Gabbar	Singh	435972.14

SBI Database

	uid	list_of_medical_conditions
1	143456789011	HIV Positive, Tuberculosis
2	123456789016	
3	123456789015	
4	123456789014	
5	123456789013	Hyperthyrodism
6	123456789012	Hypertension

NRHM database (supposedly anonymized)

Socio-economic Caste-Census DB

	uid	religion	caste	annual_family_income
1	143456789011	Christianity	NA	12000000.00
2	123456789016	Hindu	Arya Samaj	0.00
3	123456789012	Hinduism	Valmiki	4000000.00
4	123456789014	Hinduism	Kayasth	3500000.00
5	123456789013	Islam	NA	13000000.00
6	123456789015	Sikhism	NA	700000.00

The UID will become a single "handle" to all data in all databases once the databases are seeded with the UID. It is possible to "converge" the data in these different databases computationally (i.e. the proverbial "click of a button") once such an unambiguous and reliable handle is provisioned and seeded.

Converged View

	uid	first_name	last_name	religion	caste	annual_family_income	account_balance	list_of_medical_conditions
1	123456789012	Jai	Dev	Hinduism	Valmiki	4000000.00	435969.34	Hypertension
2	123456789013	Rahim	Ahmed	Islam	NA	13000000.00	435970.27	Hyperthyrodism
3	123456789014	Basanti	Dutta	Hinduism	Kayasth	3500000.00	435971.21	
4	123456789015	Gabbar	Singh	Sikhism	NA	700000.00	435972.14	
5	123456789016	Radha	Radha	Hindu	Arya Samaj	0.00	435973.07	

UIDAI – the MoUSIC Director